UTC Aerospace Systems

# Fault Detection & Isolation in Aerospace Applications:

# Understanding & Determining Technology Gaps

Richard Poisson
Technical Fellow Advanced Architecture
richard.poisson@utas.utc.com

# KEY IDEAS

Faults will always be present

Aircraft safety & availability is key to UTAS' business

Fault detection and isolation is a key part of safe flight

What is hard?

- Detecting and isolating faults without any extra instrumentation.

Making BIT more effective and more reliable

- Keeping a low False Alarm Rate (FAR)
- Lowering the No Fault Found (NFF or FNF)

What are the opportunities

- The current methods for detection and isolation currently in use have reached a plateau where the increase in detection and isolation is solely based on increased direct visibility

# PART 1 FAULTS

What they are and why we care

# TERMINOLOGY

<u>Hazards</u>:

Things that go wrong that have a negative effect on the aircraft safety

Hazards are characterized in two major ways

**Probability** - the likelihood of the hazard being realized

**Severity** - A classification on the extent of the hazard

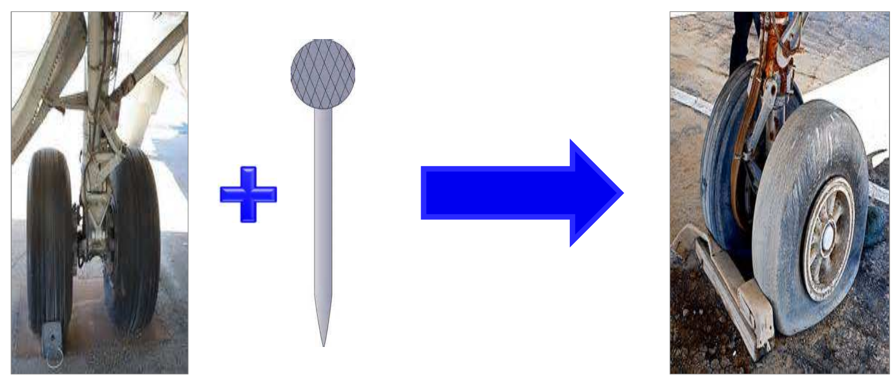
<u>Fault</u>:

Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

<u>Failure</u>:

The inability of a system to perform its required functions within specified performance requirements

| Hazard Probability | | | | |
|---|---|---|---|---|
| Per Flight Hour | | | | |
| Probability (quantitative) | 1.0 | 1.0E-5 | 1.0E-7 | 1.0E-9 |
| Probability (Descriptive) | Probable | Improbable | | Extremely Improbable |
| **Hazard Classification** | | | | |
| Failure Condition Severity Classification | Minor | Major | Hazardous | *Catastrophic* |
| Failure Condition Effect | • Slight Reduction in Safety Margins<br>• Slight increase in crew workload<br>• Some inconvenience to the occupants | • Significant reduction in Safety Margins or functional capabilities<br>• Significant increase in crew workload or in conditions impairing crew efficiency<br>• Some discomfort to the occupants | • Large reduction in Safety Margins or functional capabilities<br>• Higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely<br>• Adverse effects upon occupants | All failure conditions that prevent continued safe flight and landing |
| Design Assurance Level | Level D | Level C | Level B | Level A |

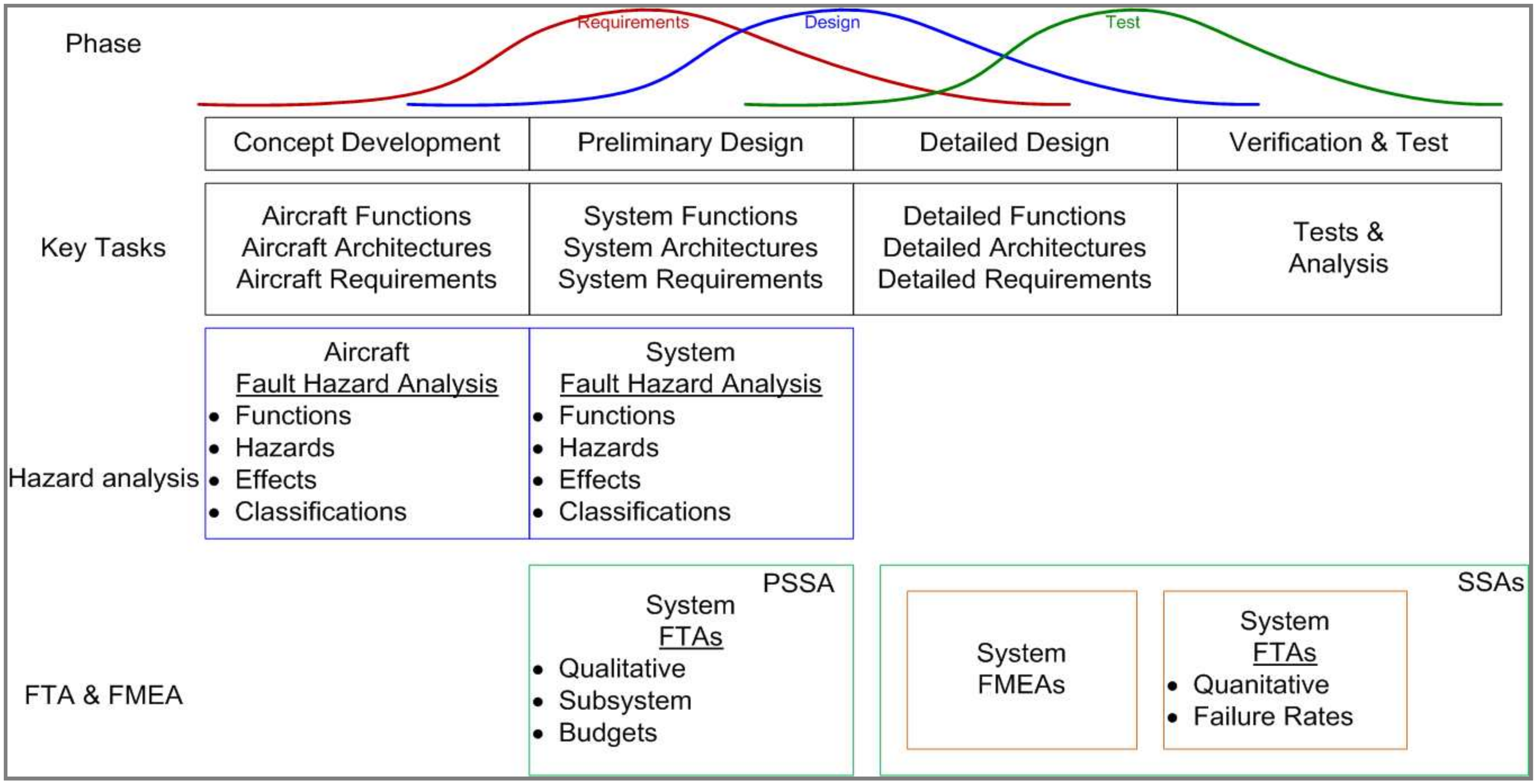
# WHY WE CARE

Safety is the #1 priority with anything that flies

Anything that is carried onboard as equipment has to be safe and <u>provide value</u> to the aircraft or its mission

Failures detract from both of these goals so we try to detect and isolate faults before they become failures


# LIFECYCLE TO ADDRESS FAULTS*




**Safety, fault identification, fault detection and fault isolation are tackled in all phases of the design and development process**

*Adapted from ARP 4761

# AEROSPACE STANDARDS

The aerospace industry has created a series of standards for design and analysis of aircraft and aircraft components

These standards describe the minimal acceptable limits for components according to the function on the airplane. These are referred to ATA chapters

*Examples*: Chapter 24: ***Electric Power***
Chapter 21: ***Air Conditioning***

In addition to the guidance on specific aircraft systems, There are general purpose specifications that help in the design, analysis and certification of aircraft components and systems

**Specifications**

| | |
|---|---|
| *ARP4754A* | *Guidelines for Development of Civil Aircraft and Systems* |
| *ARP4761* | *Guidelines and methods for conducting the safety assessment on civil airborne systems and equipment* |
| *DO-178* | *Software Considerations in Airborne Systems and Equipment Certification* |
| *DO -254* | *Design Assurance Guidance For Airborne Electronic Hardware* |

# PART 2 THE DESIGN PROCESS

How do we do it today

# UTAS 787 PROGRAM CONTENT

**Aerostructures**

Nacelle Systems

Thrust Reverser System

**Electric Systems**

Ram Air Turbine

Electric Motor Pump

Primary Power Distribution

Remote Power Distribution

Electrical Power Generating & Start System

**Landing Systems**

Wheels & Brake System


**Engine & Environmental Control Systems**

Environmental Control System

- Air conditioning pack
- Cabin pressure control
- Integrated cooling
- Power electronics cooling
- Lower pressure system
- Protective systems

Nitrogen Generation System

RR Engine Accessories

- Gearbox
- Engine Control System
- Sensor Suite

**Interiors**

Cargo Handling System

Flight Attendant Seating

Interior Lighting System

Exterior Lighting System

**Pratt & Whitney AeroPower**

Auxiliary Power System

**Sensors & Integrated Systems**

Fire Protection Systems

Proximity Sensing System

Fuel Measurement / Management Systems

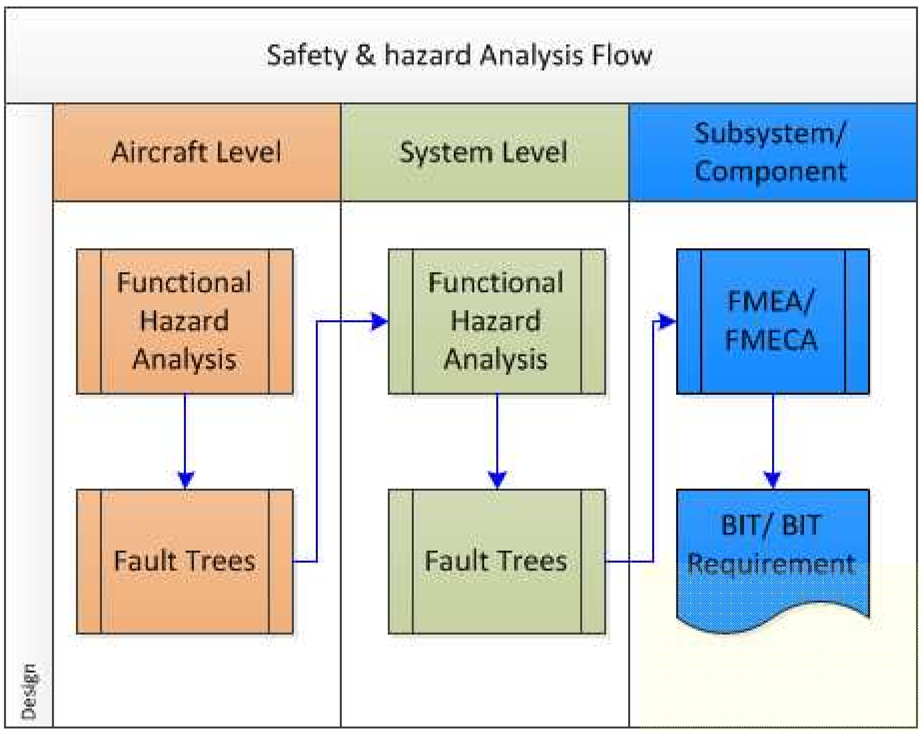
Security & Surveillance Systems

20 systems, 685 unique assemblies, >2,900 part numbers

# KEY POINTS

The process and methods of analyzing the safety aspects of a system are well documented

It follows methods and tools  laid out in the *“Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment” (Arp 4761)*

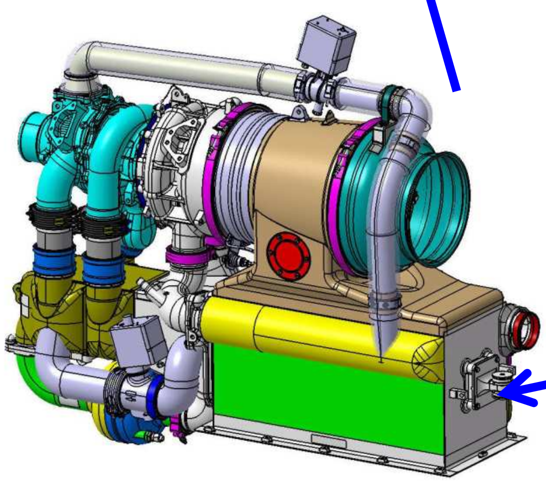



ARP 4761  describes guidelines and methods of performing the safety assessment for certification of civil aircraft. It is primarily associated with showing compliance with FAR/JAR 25.1309. The methods outlined identify a systematic means to show compliance.

The concept of Aircraft Level Safety Assessment is introduced and the tools to accomplish this task are Outlined along with the aircraft’s operating environment

This is where the detection and Isolation methods and tools are used

# SYSTEMS, SUBSYSTEMS & COMPONENTS



Aircraft Cabin Air Conditioning Temperature Control System (CACTCS)

<u>System</u>

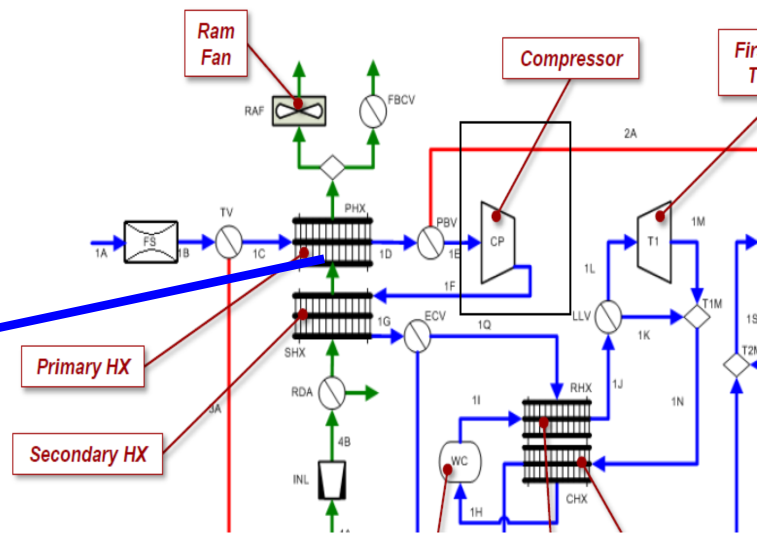
Environmental Control System

<u>Sub-System</u>

Air conditioning pack

<u>Component</u>

Primary Heat Exchanger



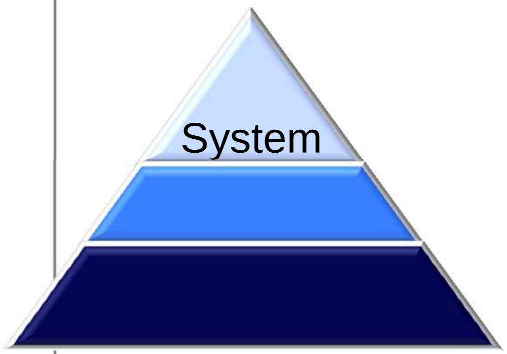

Primary Heat Exchanger

Contains no technical data
Cleared for Public Release in accordance with UTAS-LCC-PRO-0907

# STEP 1 DETERMINING THE HAZARDS

Simple example for a notional cabin air temperature control system

| ID | Function | Hazard description | Failure condition ( effect of hazard on airplane) | Verification Approach | Severity |
|---|---|---|---|---|---|
| 1 | Temperature Control | Malfunction of Air Conditioning System creating excessively hot supply air to cabin and/or flight deck and inability to shut off the heat source | Failures within the Air Conditioning system create high supply air temperatures to the flight deck and/or cabin resulting in excessively warm flight deck and/or cabin, and packs do not respond to crew OFF selection.<br>May cause incapacitation of flight crew or severe physical distress such that the crew could not be relied on to perform its tasks. Potential prevention of continued safe flight and landing of the aircraft. Possible adverse impacts to some occupants, including multiple passenger fatalities. May cause failure of electronic equipment including flight critical equipment. | FTA, FMEA, Analysis/ Design Review | Catastrophic |



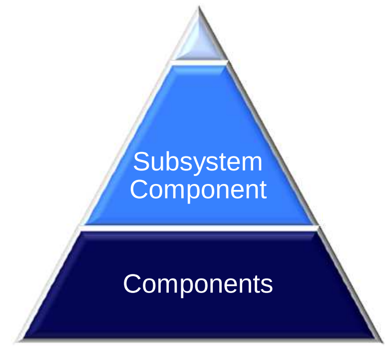

The Hazard Analysis identifies failures that must be prevented and identified

Hazard prevention begins with the detection and the isolation of the faults that would lead to the hazard

The **Failure Modes Effects Analysis** and the **Failure Modes Component Effects Analysis** are used to explore the faults

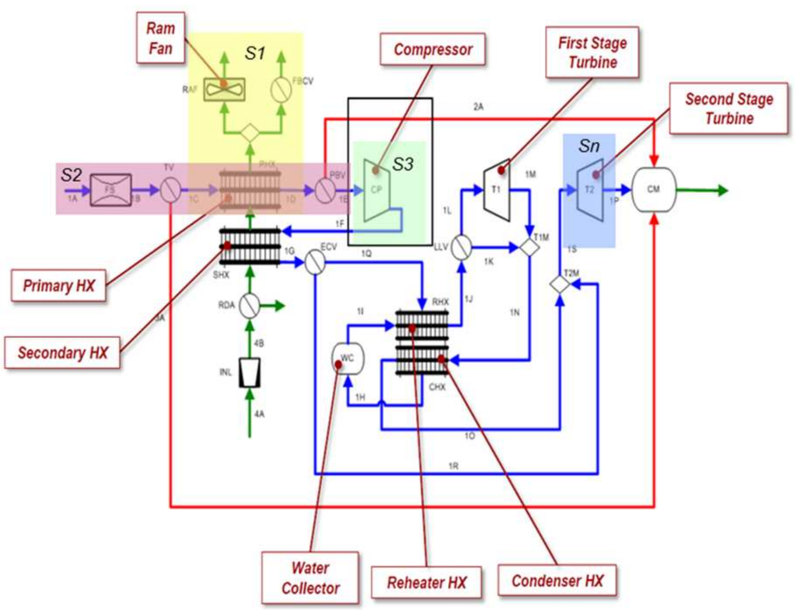
# STEP 2 FAILURE MODE EFFECTS ANALYSIS

## Subsystem and component




**Failure Modes & Effects Analysis** (FMEA) lists the faults and determines if they are observable at the system and subsystem level

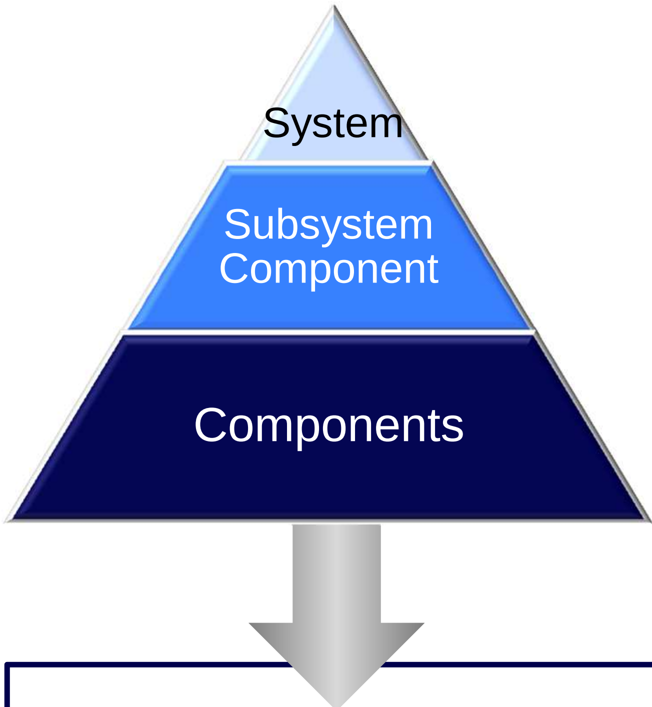
**Failure Modes & Effects Component Analysis** (FMECA) lists the faults and determines if they are observable at the component level




Sample faults identification

| ID | System Fault |
|---|---|
| S1 | Primary Ram Flow not Available |
| S2 | Loss of Bleed flow to Compressor |
| S3 | Pressure loss at CP |
| Sn | Turbine stage 2 non operational |
| **ID** | **Component Fault** |
| C1_1 | Ram Fan Bearing Fault |
| C1_2 | Ram Fan Motor Fault |
| C1_3 | Ram Fan Flow Control Valve Fault |
| C1_n | Ram Fan Door Fault |
| C3_1 | Compressor Bearing Fault |
| C3_2 | Compressor Blade Fault |
| C3_3 | Compressor inlet Fault |
| C3_n | Compressor outlet Fault |

# RESULTS FROM THE ANALYSIS




Hazard Analysis

Subsystem Level Failure Mode and Effects Analysis ( FMEA)

Failure Mode and Effects Component Analysis (FMECA)

The results from the Hazard Analysis, FMEAs, FMECAs determine what faults need to be observable and isolatable

This forms the basis of the requirements for fault detection and fault isolation

# FAULT ISOLATION

Determining that a fault is present is not enough.  Before the fault results in a failure, it needs to be Isolated.  The act of isolation is critical to

- Safety
- Maintenance
- Accommodation (living with faults)

The industry has set a very high bar for fault detection and isolation.

Typical requirements:

- 100 % to 3 Line Replaceable Units of a system
- 98% to a Single Line Replaceable Unit in a system or subsystem
- 95% to a single sub component in a subsystem

***What can we do to help with the Fault detection and Isolation so that we can catch faults early, before failures ?***

# CHALLENGES: FAULT DETECTION & ISOLATION

Systems are becoming more intelligent and behavior can not always be predicted

Causal relationships of systems and faults are not well known for complex systems

False positives annoy people and result in lost confidence in the system's ability to predict the fault (crying wolf)

False negatives (don't detect when there is a fault) big factor in safety critical systems (better to be a crying wolf, sometimes)

The extra weight, cost and reliability of the added hardware and software for detection and isolation deters inclusion onto platforms

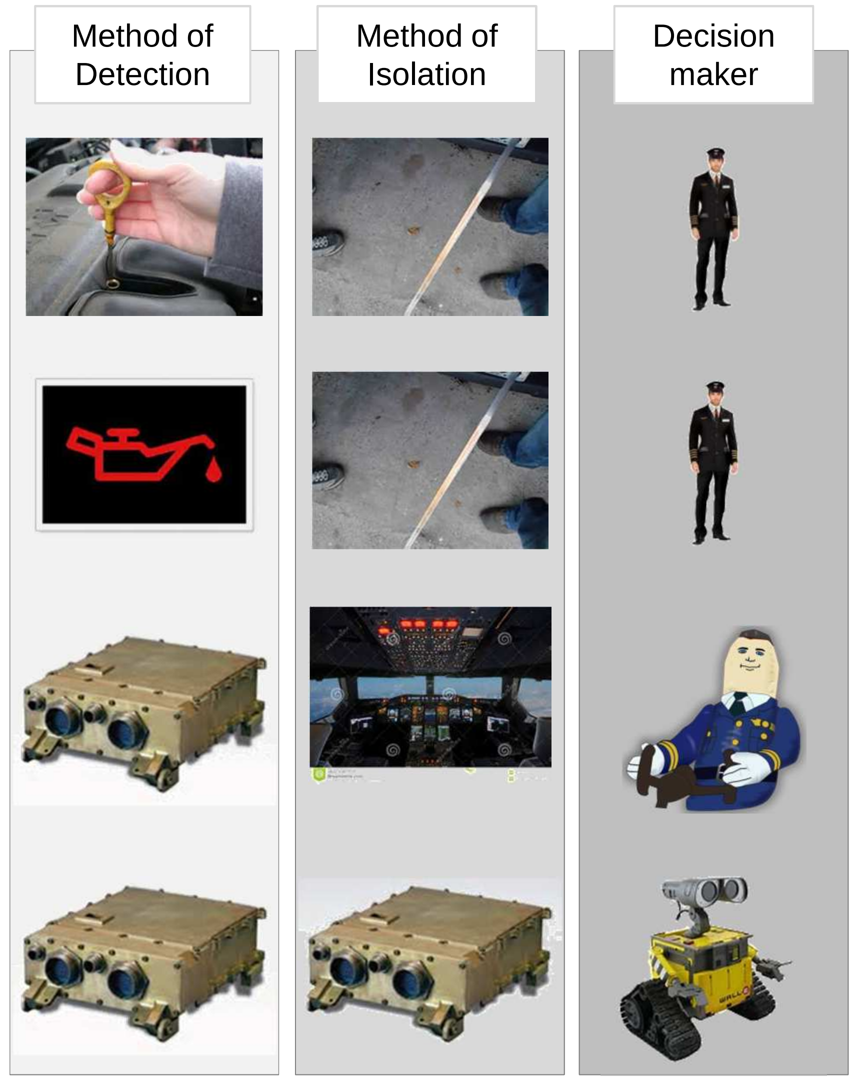
# FAULT DETECTION & FAULT ISOLATION

Mechanical systems and mechanical monitors. Faults were harder to find and diagnose Go/NoGo criteria was up to the decision maker. The user had limited visibility to the system and to the interaction between systems

With the addition of electronics,
the monitoring became concentrated and remote. The Go/NoGo decision was still up to the decision maker. Some interaction could now be monitored

Digital Control and Intelligent Systems,
The decision maker is notified but the corrective action is accomplished without intervention

Autonomous Control and Operation Detection Isolation and accommodation all performed without notification (there will be a log)



# PART 3 BIT AND BITE

Implementing Detection and Isolation

# KEY POINTS

Once the hazards have been identified, the list of faults have been created, the process shifts to implementing of the detection and isolation these faults

BIT and BITE is the terminology that is used for the implementation of fault detection and isolation methodology

BIT detection and isolation  takes place in all phases of flight and ground operations

BIT effectivity directly relates to the aircraft safety and availability

# DEFINITIONS

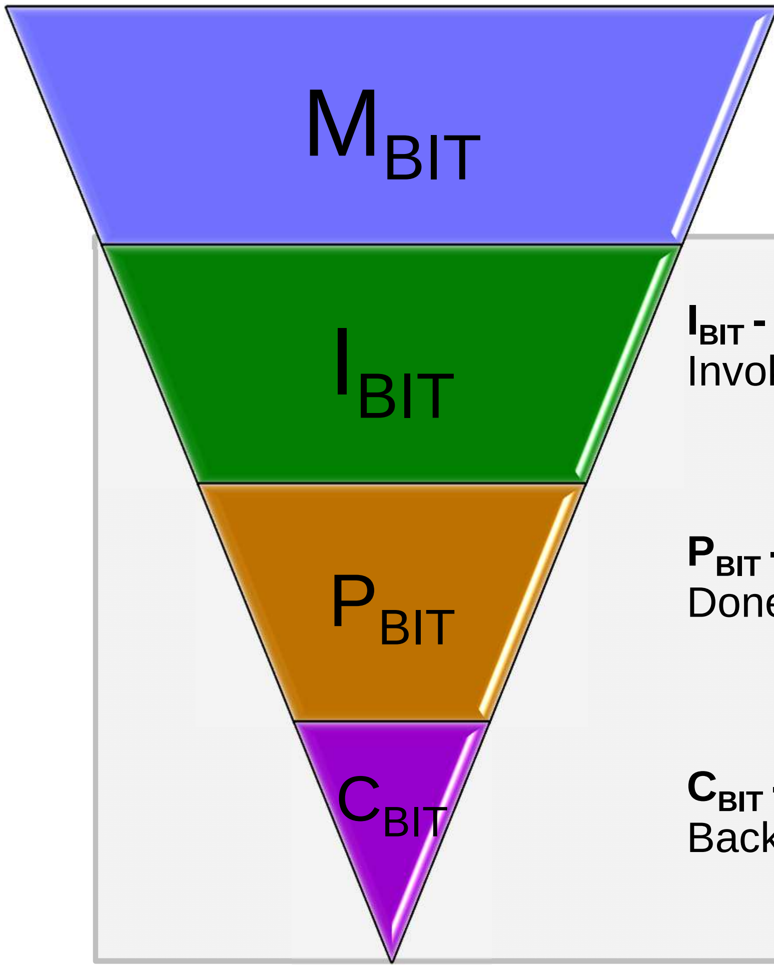
***BIT***

**Built in Test** – usually software that checks the health of a system / component(s) by setting and measuring key parameters during operation. It is the logic that identifies and isolates the faults.

***BITE***

**Built in Test Equipment** – hardware whose sole purpose is to perform BIT operations.

# BIT PYRAMID




**$M_{BIT}$ -Maintenance BIT**
Used when special equipment is connected or a special diagnostic mode is entered

**$I_{BIT}$ - Initialization BIT**
Invoked by specific commands

**$P_{BIT}$ - Power on BIT**
Done at cold start

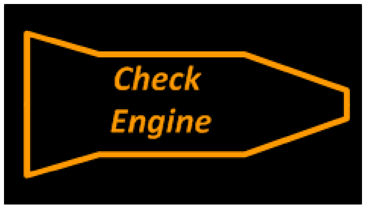
**$C_{BIT}$ - Continuous Bit**
Background /Foreground

ODB2 Scanner

Self Test on Smoke detector

PC POST Memory Test

Check Engine Indicator




**Typically systems have all 4 types of BIT designed. The effectiveness of each determines the quality of the detection and isolation**

# PART 4

Why we need more focus and research

# KEY POINTS

Faults will never be eradicated. There will always be System, Mechanical, and Electrical faults. But in the age of Cyber-physical systems we also have:

- Software faults, algorithmic faults, variability in all forms
  - The trend is towards more electric, more integrated and more intelligent aircraft systems
  - Highly integrated and intelligent systems leads to highly complex behaviors
  - The current methods for detection and isolation currently in use have reached a plateau where the increase in detection and isolation is solely based on increased direct visibility

**What do we get for all these intelligent and integrated systems?**

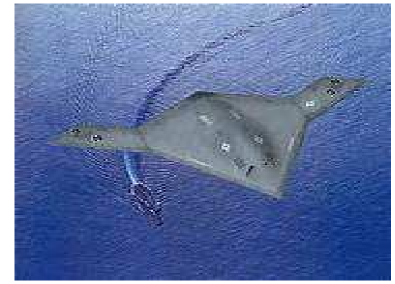
# INCREASED CAPABILITIES

## Growth in the capabilities &efficiency

1915

1945

2015



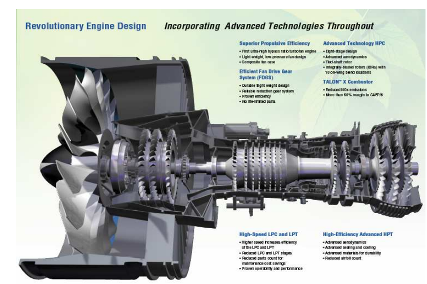
2025?

1960s

1970s

2009

2016




*But with added capabilities come →*

# ADDED COMPLEXITY

## 1970-80 Cockpit

Every gauge is unique

Every indicator is unique

Numerous equipment including wire and connections.

Limited by the size of the cockpit

Grouping not always logical

Extremely difficult to add capability

Hard to monitor- more staff required

## 2014 Glass Cockpit

Multi-function Displays

Logical grouping of signals

Reduces pilot scan area

Reduced wiring ( networked)

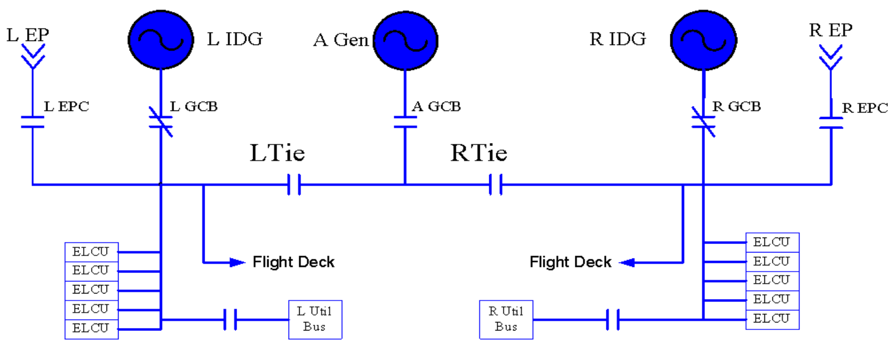
Easy to add capability

Large dependence on electronics and software

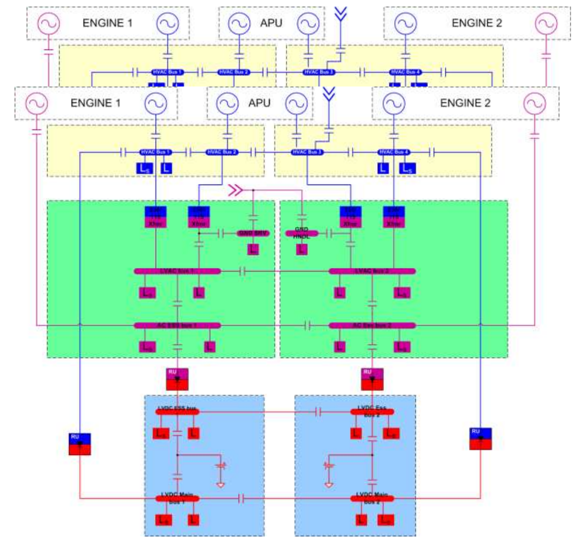
# ELECTRIC POWER

## Generation / Distribution

Conventional Aircraft




More electric aircraft




| Conventional | Key Feature | More Electric |
|---|---|---|
| 5 | Sources of power | 7+ |
| 3 | Distinct power busses | 12 |
| 9 | Power control contactors | 30 |
| 4+ | Control processors | 10+ |
| <200 KW | Total power output | >1 Meg W |
| ~2^12=4096 | Physical configurations * | ~2^30 = 1,073,741,824 |

*Physical system constraints will reduce this number

# WHAT'S THE BENEFIT

Increased system safety

More efficient maintenance

Shorter downtime

Lower false alarm rate (FAR)

Better response to actual faults

Longer availability

Longer time on wing

Accommodation

# HOW TO GET WHERE WE NEED TO BE

## Minimize BITE

<u>What?</u>

Better/New IBIT, CBIT, PBIT algorithms tools and methods

<u>Why?</u>

Limited visibility into the system

Use relationships between what can be measured and what can be inferred

Reduced False alarm rate

- Currently >50% in the industry
- Reduced NFF for failures Identified

<u>How?</u>

Learning algorithms

Anomaly detection that is “in the loop”

Model-based Detection & Isolation

# HOW TO GET WHERE WE NEED TO BE

<u>Constraints / challenges:</u>

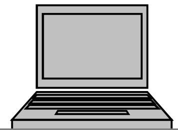
Limited computational resources

Skill level of current workforce

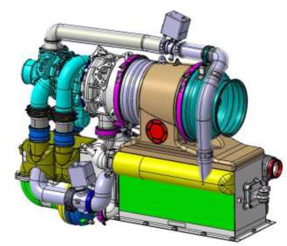
Mostly BS and MS with some PHD

System integration encompassing mechanical, electrical, and software control systems.

Model Based fault detection & isolation is not yet at the technology readiness level for certified flight



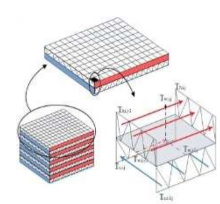
| Current state laptop | Key feature | Current state integrated control unit |
|---|---|---|
| 4+ | CPU/Core | 1 |
| Storage unlimited | Program Memory | 4MB-256M |
| 4-16 GB | RAM | 256K – 256M |
| 3+ Ghz | Clock Speed | 600 MHz |

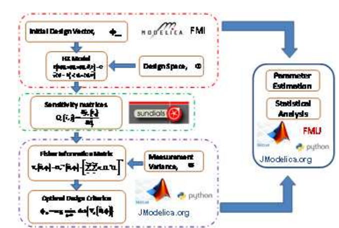


Electrically driven compressor

Software controlled motor drive

Networked power distribution

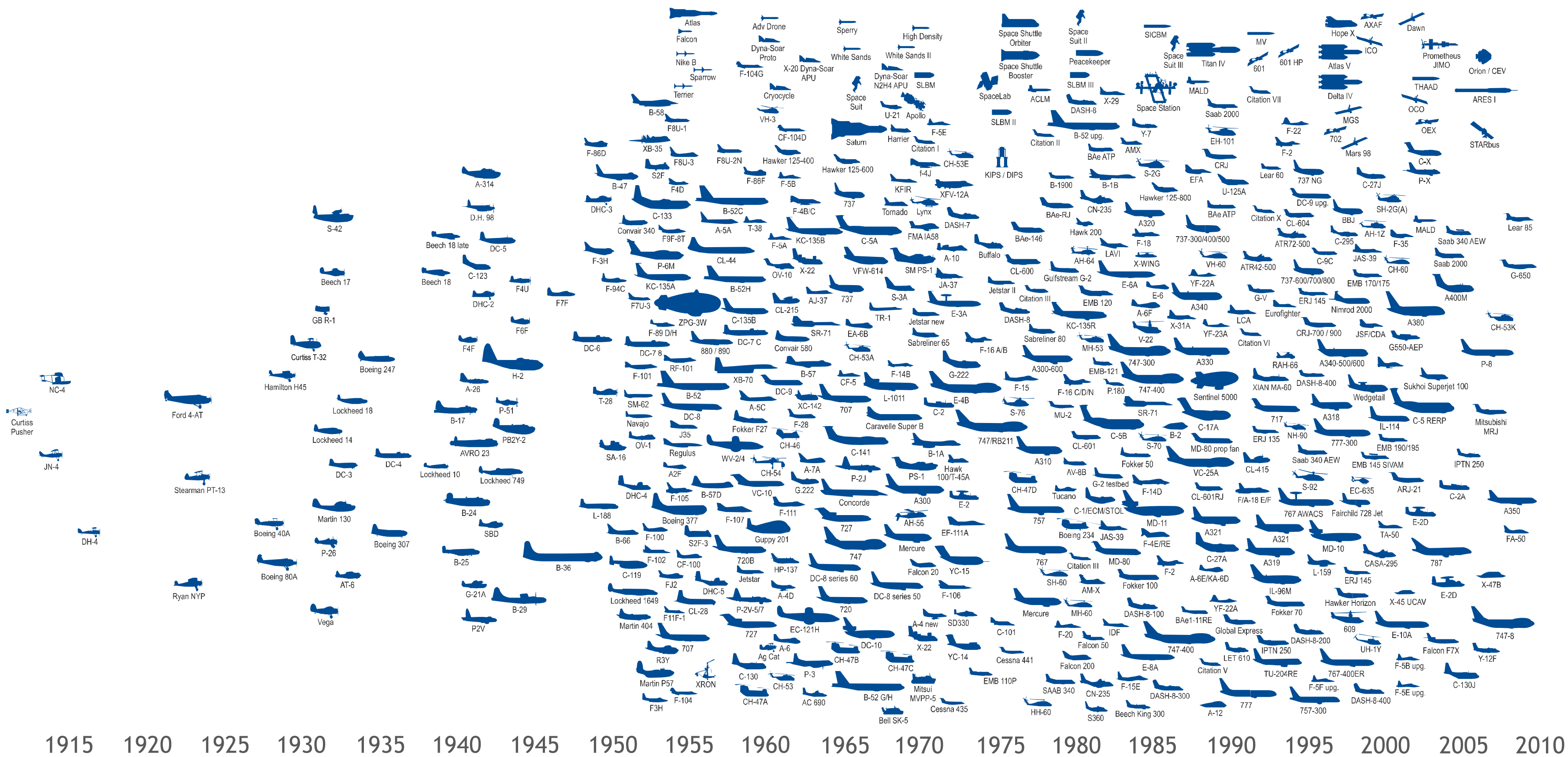




Dr. George Bolas and Kyle Palmer University of CT.

# OPPORTUNITIES

## Experience 1900's – today




***UTAS is on almost every Platform that flies !***

# CLOSING REMARKS

WHO

Where are the solutions going to come from?

- ☆ Industry
- ★ Academia
- ★ Partnerships between Industry and Academia
- ★ Government Sponsored Research

IASE is ideally suited to tackle these challenges

*Remember*

*This is  a topic that has all the industry watching*