Delta System Solutions

A White Paper:

Zonal Safety Analysis in Aerospace: what it is and why we do it

This is 1 from a series of 3 white papers covering the Common Cause Analysis techniques: CMA, PRA and ZSA.

Author: Lucas Pereira
Info@delta-system-solutions.com

INTRODUCTION

The ARP4761[1] describes guidelines and methods for performing safety assessments of aircraft, systems and equipment, supporting compliance with certification requirements. It is applicable to new designs or to modifications to existing designs.

The safety assessment process provides a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazard have been properly addressed. It also provides confidence that the likelihood of failures and errors that may lead to failure conditions has been minimized.

For integrated systems, the safety assessment process should take into account any additional complexities and interdependencies which arise due to integration.

Independence between functions, systems or items may be required to satisfy the safety requirements. Therefore, it is necessary to ensure that such independence exists, or that the risk associated with dependence is deemed acceptable.

The Zonal Safety Analysis (ZSA), along with the Particular Risks Analysis (PRA) and Common Mode Analysis (CMA), provides a method for evaluation of independence and generation of independence requirements.

1. WHAT IS ZONAL SAFETY ANALYSIS?

A ZSA is performed on each zone of the aircraft to ensure that the design and installation of systems and equipment complies with the safety requirements with respect to:

- the basic installation;
- the interference between systems and equipment;
- maintenance errors.

The ZSA is intended to identify whether there are any zonal issues that could compromise the independence principles.

The ZSA is carried out during the whole development process:

- during the Preliminary Aircraft Safety Assessment / Preliminary System Safety Assessment (PASA/PSSA) to generate physical installation requirements;
- during the Aircraft Safety Assessment / System Safety Assessment (ASA/SSA) to verify the installation requirements.

The ZSA is predominantly an aircraft and engine level analysis. However, it is also conducted at lower level, on sub-systems, driven by higher-level requirements.

The Figure 1 depicts the ZSA, as part of the Common Cause Analysis (CCA), in the "V-Model" development process.

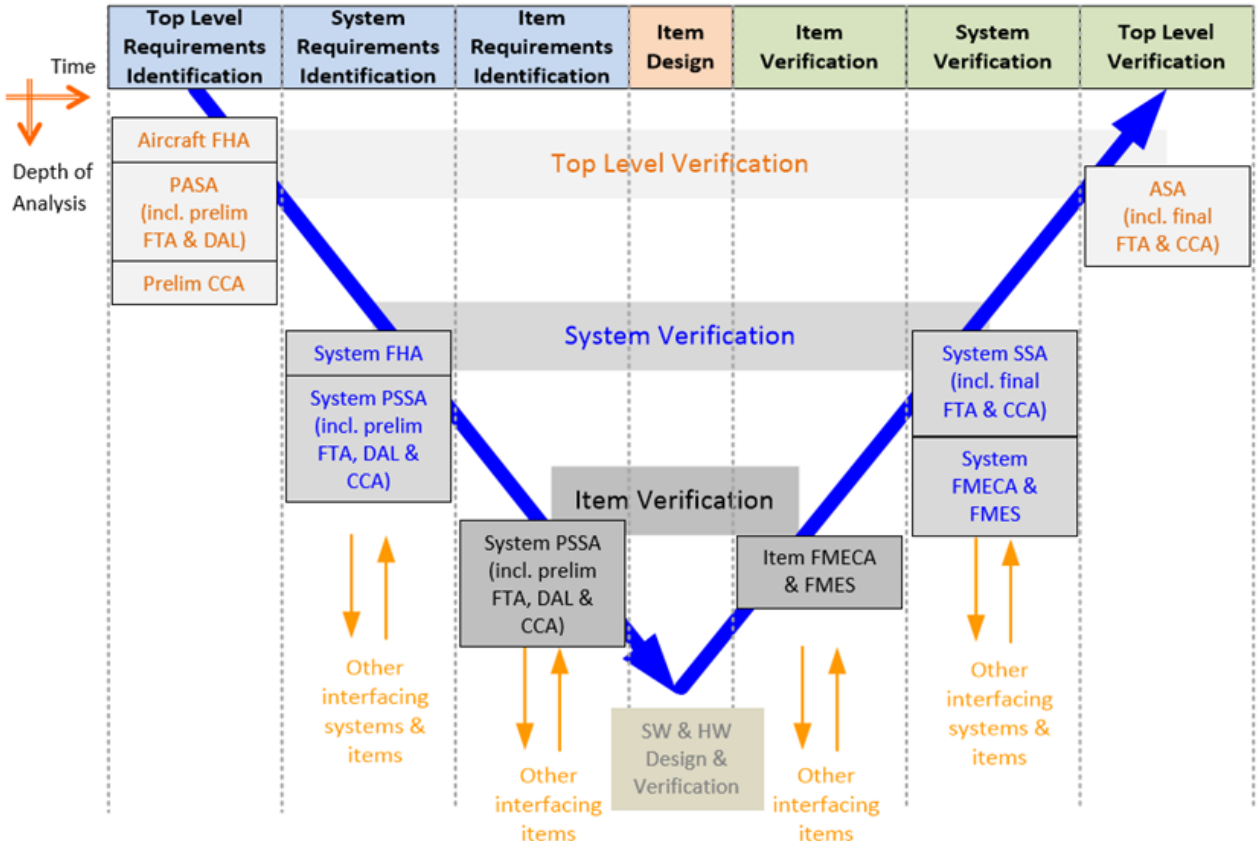

Figure 1. V-Model for safety process in the aircraft development

1.1 ZONAL SAFETY ANALYSIS PROCESS

As an input for the ZSA, design and installation guidelines should be prepared for each new project. The guidelines are mainly composed of data accumulated on previous programs. It should consider also aircraft level requirements and considerations from the PASA/PSSA, as well potential maintenance errors. Additionally, a list should be created (usually based on the FMEAs and on the

known intrinsic hazards) to identify physical hazards inherent to the system/equipment potentially having external effects.

In order to perform the ZSA the aircraft should be partitioned into zones. The zones can be established in the scope of the ZSA or be based on other partitioning already defined for the aircraft. However, the zones should present similar environmental characteristics, in particular regarding pressure, temperature and presence of flammable fluids. Usually, sub-zones are also defined.

An installation questionnaire and checklist should be prepared to support the Zonal inspections, considering general checkpoints, system specific design and installation checkpoints or zone specific design and installation checkpoints.

Zonal inspections can be done either with drawings, computer-based models or physical installation. Usually Digital Mock Ups (DMU) are used to assess the proposed design during the development phase. Inspections in the early production aircraft should also be performed in order to verify that the intallations requirements are meet.

2. WHY DO ZSA? (THE TWA 800 ACCIDENT)

To highlight the value of ZSA, this accident had the potential to be prevented by conducting a systematic and comprehensive ZSA in accordance with today's standards and guidance.

On July 17, 1996, the Trans World Airlines (TWA) flight 800, a scheduled international passenger flight from New York to Paris, operated by a Boeing 747-100 series airplane (model 747-131), crashed in the Atlantic Ocean near East Moriches, New York, 12 minutes after takeoff from John F. Kennedy International Airport (JFK). All 230 people on board were killed, and the airplane was destroyed.

the CWT that allowed excessive voltage to enter it through electrical wiring associated with the Fuel Quantity Indication System (FQIS).

A major reason for the flammability of the fuel/air vapor in the CWT on the 747 was the large amount of heat generated by the air conditioning packs located directly below the tank, which significantly elevates the temperatures in the pack bay. Heat from the pack bay could be transferred to the CWT through the bottom of the tank and caused temperatures to rise above the lower flammability limit.

On the day of the accident, the CWT contained about 300 pounds of fuel. Additionally, the airplane remained with the

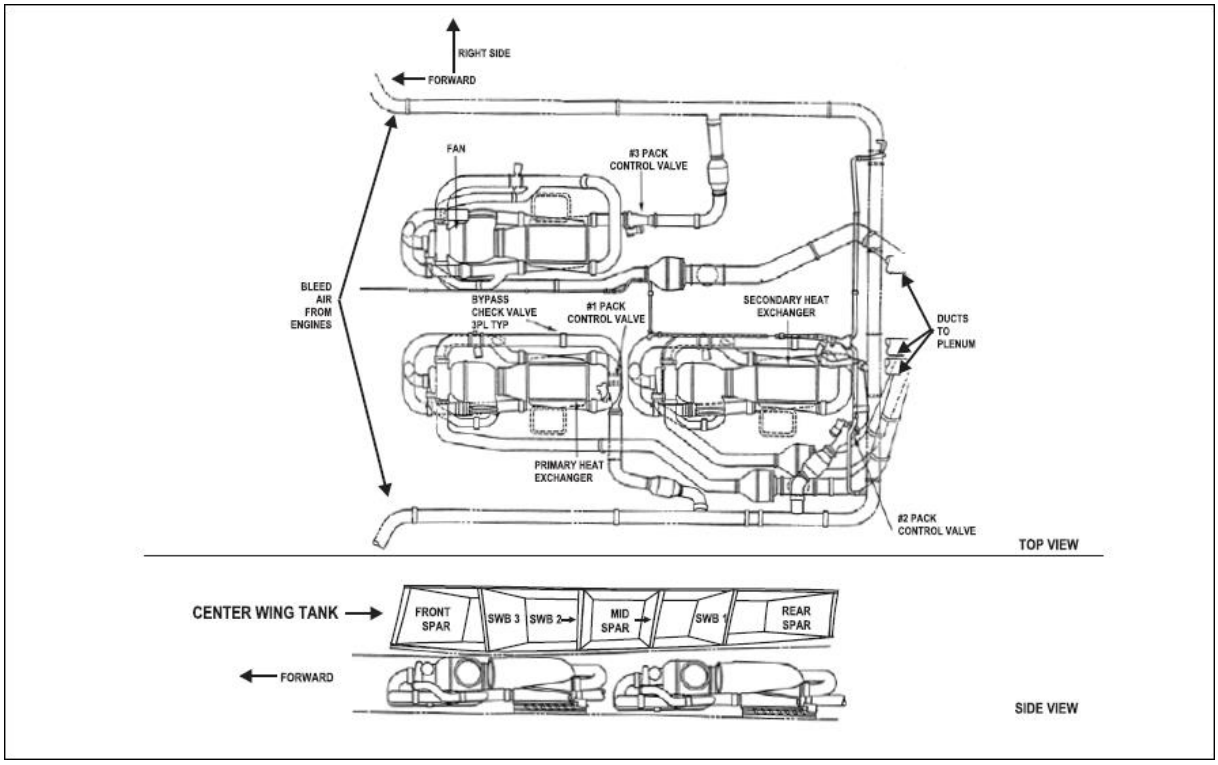

Figure 2. Top and side views of the 747-100's wing center section and air conditioning system.

The National Transportation Safety Board[2] (NTSB) determined that the probable cause of the TWA flight 800 accident was an explosion of the Center Wing Fuel Tank (CWT), resulting from ignition of the flammable fuel/air mixture in the tank. The source of ignition energy for the explosion could not be determined with certainty, but the most likely was a short circuit outside of

auxiliary power unit (APU) and two of its three air conditioning packs operating (for about 2 1/2 hours) until it departed, due to a disabled piece of ground equipment and a passenger/baggage mismatch.

Flight tests indicated that fuel vapor temperatures within the CWT at the time of the accident ranged from 101°F (38.3°C) to

127°F (52.8°C). Further tests showed that Jet A fuel vapors under conditions simulating the pressure, altitude, and fuel mass loading of TWA flight 800 are flammable at these temperatures and at those as low as 96.4°F (35.8°C).

The only electrical wiring located inside the CWT was the wiring associated with the FQIS. According to the design specifications, the voltage to the FQIS wiring was limited so that it could not discharge energy in excess of 0.02 mJ. However, excess voltage from a short circuit could be transferred from wires carrying higher voltage to wires carrying lower voltage if the wires were near each other. The investigation found that the design specifications permitted FQIS wiring to be bundled with, or routed next to, higher-voltage airplane system wires, some carrying as much as 350 volts.

As a result of the investigation of the TWA flight 800 accident, the NTSB issued a list of recommendations to the Federal Aviation Administration (FAA), mostly related to fuel tank and wiring-related issues.

During ZSA, influence of the heating sources in the surrounding equipment should be assessed, especially for zones containing flammable fluids. The wiring installation should also be assessed, considering hazards resulting from wiring degradation, open circuits and short circuits.

3. REFERENCES

[1] **SAE International (1996).** *ARP4761: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment.* 400 Commonwealth Drive Warrendale, PA, United States.

[2] **National Transportation Safety Board. 2000.** *In-flight Breakup Over The Atlantic Ocean, Trans World Airlines Flight 800, Boeing 747-131, N93119, Near East Moriches, New York, July 17, 1996.* Aircraft Accident Report NTSB/AAR-00/03. Washington, DC.