Application of FAR XX.1309
BK117 External Fuel Tanks

David Weston, Airwork (NZ) Ltd
2017 DDH Seminar

airwork
(NZ) LIMITED

airwork

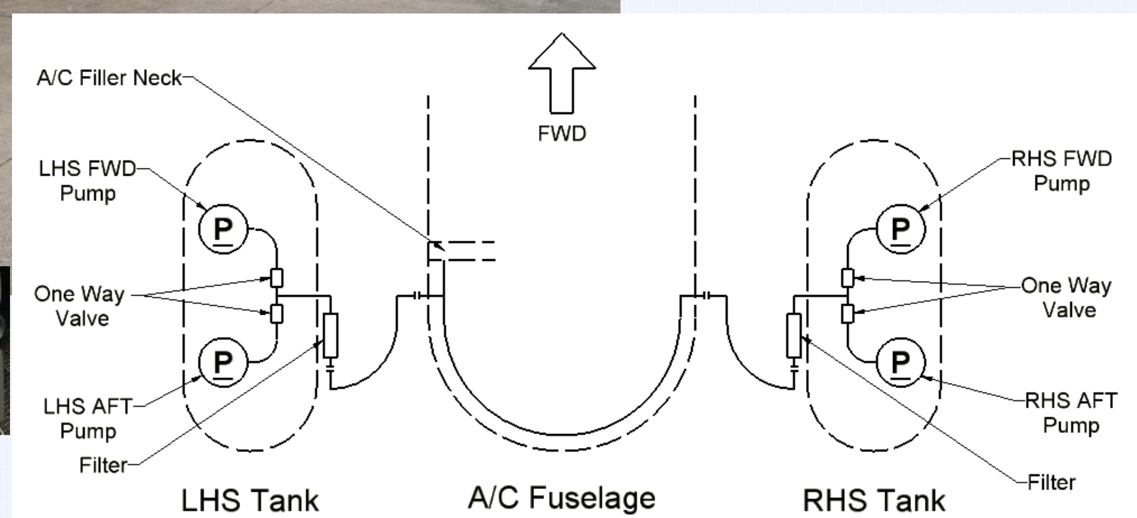
System Overview

Main tank = 700 *l*

Ext. tanks = 200 *l* (ea.)

Pilot controlled 'top-up' system.

Incl. *Main Tank Full* annunciation.



Product History & Case Study

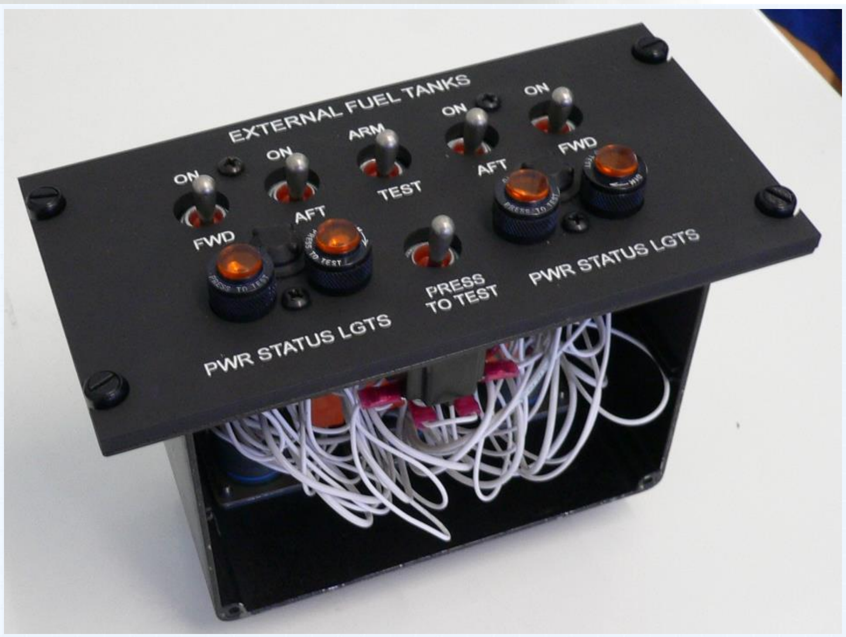
- Early versions of the fuel tank system certified as a modification ~ 1997.
- Most recent New Zealand STC approval ~ 2012.
- Operating in New Zealand, Australia, South Africa, Bolivia…..and probably others.
- Multiple evolutions to enhance pilot controls, functionality and NVG compatibility.
- Kawasaki BK117: Transport Category Rotorcraft, FAR 29 Amendment 16 (*1978*)

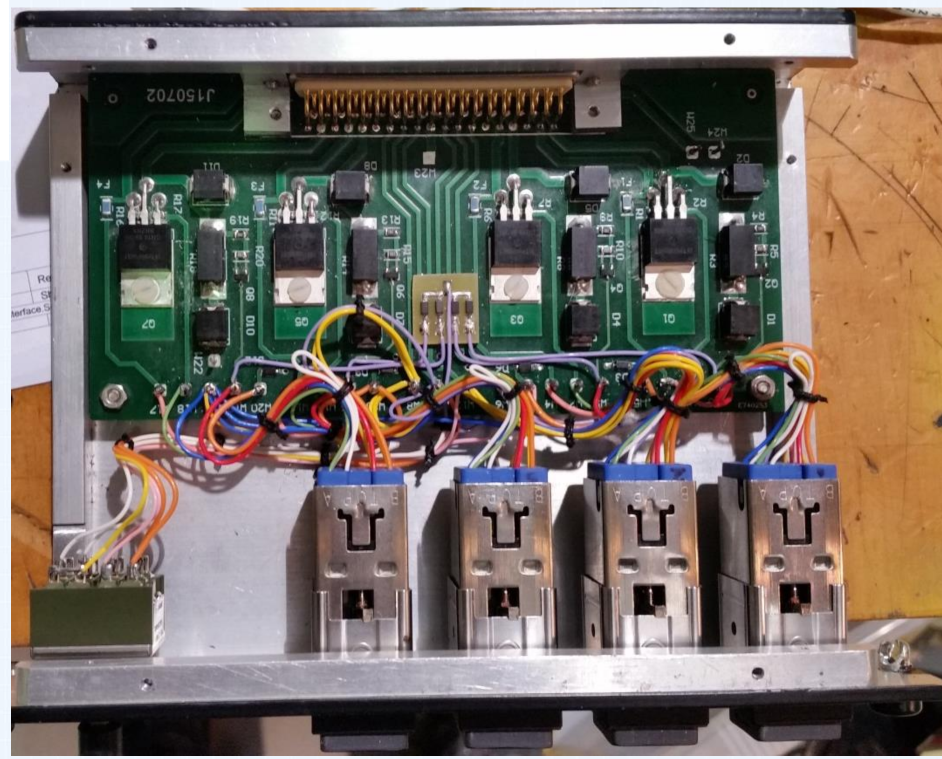
TODAYS CASE STUDY (circa. 2017):

FUEL CONTROL PANEL ENHANCEMENTS & 29.1309

- Design Change: Upgrade to Fuel Control Panel [*System*].
- Certification: One-off Serialised NZCAA Major Mod.
- Cert Basis: Per TCDS consider 29.1309 amendment 29-14.
- How did 1309 requirements influence system design, operation and certification?

Fuel Control Panel – Old and New





Flight Deck Location

Flight Manual - Operational Procedures

airwork NZ LIMITED	Document Number:	AW1344A FMS	Revision:	0
	Document:	FLIGHT MANUAL SUPPLEMENT		
	Design Change Title:	BK117 Alternate Auxiliary Fuel Tank Wiring		
	Prepared by: DR Wollen	Date: 20/01/2017	Checked by: D Weston	Date: 27/01/2017

SECTION 2. LIMITATIONS

2.1 Operations

2.1.1 If dual auxiliary fuel tanks are installed transfer of fuel to main tank must take place from both auxiliary fuel tanks simultaneously.

2.1.2 Use of both pumps (forward and aft) in each tank simultaneously to transfer fuel from an auxiliary fuel tank is prohibited.

2.1.3 All on-route range and endurance determinations must be made based on the amount of useable fuel in the main rotorcraft's tanks.

2.1.4 Flight route planning must include sufficient decision points to ensure sufficient fuel reserves are in the main rotorcraft's tanks.

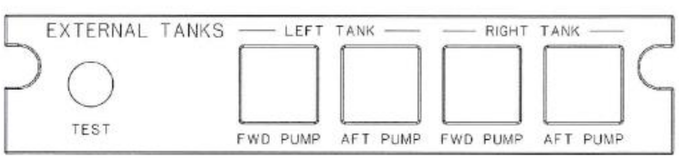
2.1.5 The only fuel transfer procedures approved are those defined in §4.4. Leaving the fuel transfer pumps ON until the main rotorcraft annunciator panel amber "MN TK FULL" light is illuminated **IS PROHIBITED**.

WARNING:

WITHIN 2 SECONDS OF FUEL OVERFLOW ANNUNCIATION OVER PRESSURIZATION OF THE ROTORCRAFT MAIN FUEL TANKS WILL OCCUR AND MAY RESULT IN DAMAGE TO THE SURROUNDING FLOOR AND SUBSTRUCTURE.

2.2 Placards

2.2.1 On the centre console – external fuel tank controller.



- External tanks 'top-up' main tanks.
- Flight Manual mandates 'decision points' during flight planning phase.
- On-route range/endurance always based upon useable fuel in main fuel tanks.
- Ensures that at any point during flight there is sufficient fuel in main fuel tanks to reach a safe landing point.
- Reasonable Procedure? Acceptance by CAA & Chief Pilot prior to approval.
- System Safety Assessment assumes 100% probability flight crew will comply with Flight Manual limitations.

1309 Approach (1 of 4)

- FAR 29.1309(a) Function and Reliability:
  - ***Required* equipment, systems and installations** *must perform intended function under any foreseeable operating condition.*
  - *External fuel tanks are not required equipment……job done?*

- FAR 29.1309(b) Hazards:
  - ***The equipment, systems and installations*** *must be designed to prevent hazards to the rotorcraft if they malfunction or fail.*
  - *Integrated Systems are selfish….. "If I'm going down I'm going to take you down with me!"*

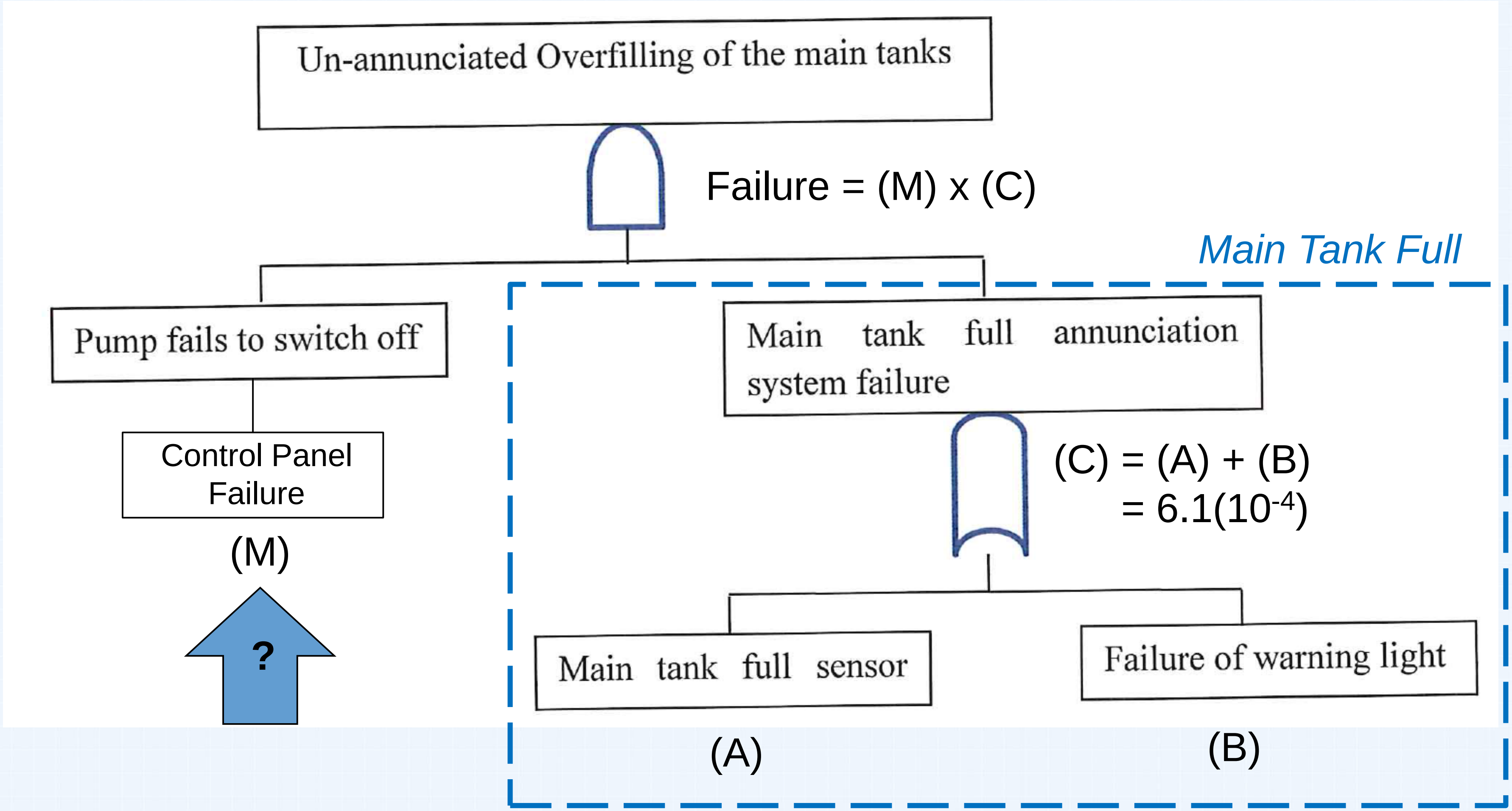
- STEP 1: Functional Hazard Assessment (FHA)
  - Top Down Approach: Consider system functionality w.r.t. flight operations.
  - In other words…..What are the potential hazards from the pilots perspective?
    - How does the pilot use the system; initial flight planning to on-route fuel transfers?
    - What are the Flight Manual procedures and what decisions does pilot have to make?
    - Are the procedures reasonable pilot workload….offshore IFR operation at night?
    - Following failure [*of external fuel tanks*] need sufficient fuel in main tank to land safely….could be offshore.

1309 Approach (2 of 4)

- STEP 1 (cont): FHA Identified TWO primary hazards.
  - FUEL IN EXTERNAL TANK(S) IS UNAVAILABLE.
    - Multiple potential causes, not assessed in detail (FHA is top down).
    - Detectable failure (failure annunciators & main tank fuel gauges).
    - On-route fuel transfer procedure ensures main tanks always contain sufficient fuel for safe landing.
    - Failure classified as **MINOR** …..”*crew actions well within their capabilities, slight increase in crew work load such as routine flight plan changes*”
    - **System** failure rate must be **$<10^{-3}$**.
  - OVERFILLING OF MAIN TANKS.
    - Multiple potential causes, not assessed YET.
    - Latent failures….pilot has no obvious indication that fuel being pumped into already full main tanks.
    - Result: Loss or fuel (vented overboard) OR over pressurisation of main tanks.
    - Failure classified as **MAJOR** …..”*significant reduction in functional capability of rotorcraft, significant increase in crew workload (emergency landing)*”
    - **System** failure rate must be **$<10^{-5}$**.

→ **COMPLETE SYSTEM, NOT JUST CONTROL PANEL.**

- STEP 2: Fault Tree – Calculate Complete System Failure Rate



airwork

1309 Approach (last one…..promise!)

Control Box - Failure Rate

- **90x components**; diodes, transistors, resistors, CBs, fuses..etc.
- PCB mounted with D-SUB connector.
- 4x Annunciator switches (int.logic).

FAULT TREE ANYONE?

Complex & Tedious.

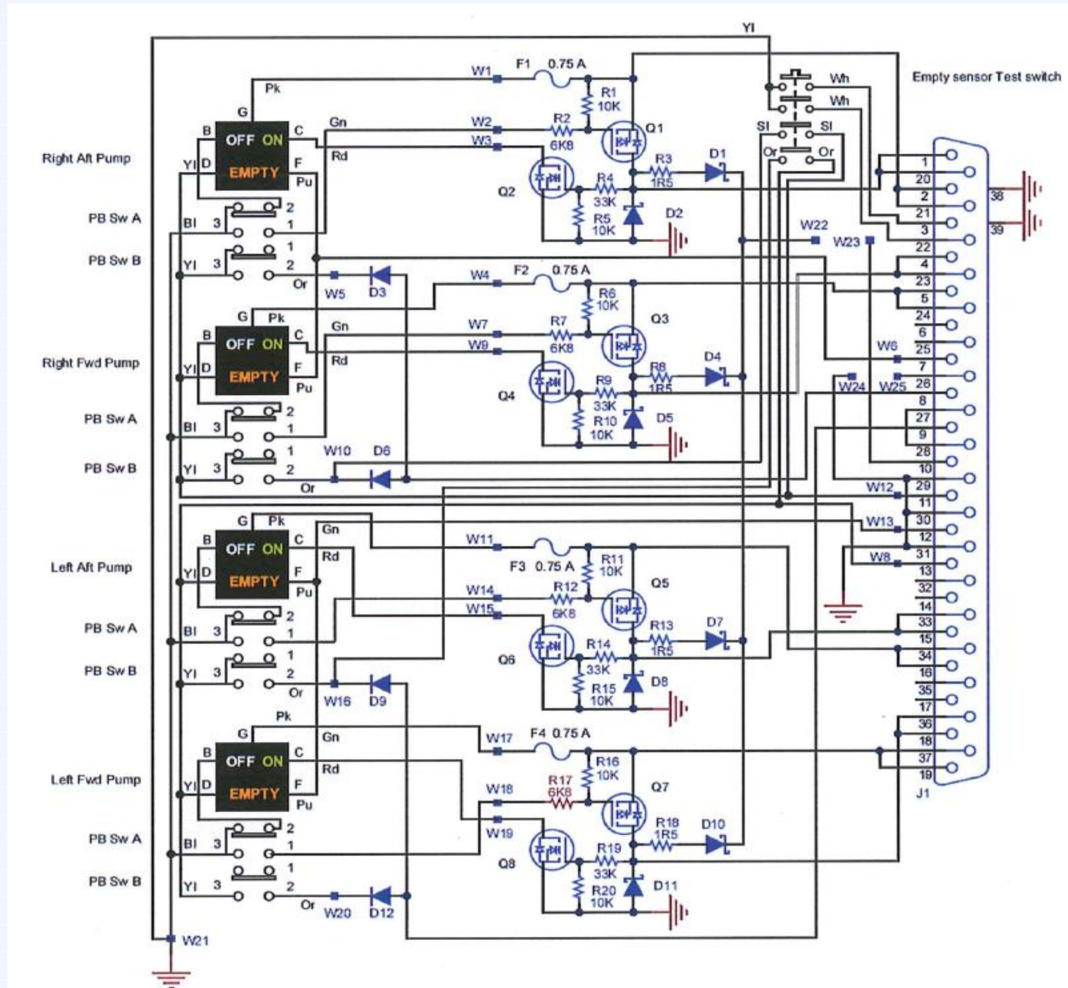
- Parts count reliability method (MIL-HNDBK-217).
- Sum failure rates of components.
- Accounts for PCB and soldering.
- Simple/conservative method.
- Failure rate (M) = $4.2(10^{-4})$

THE ANSWER…….

Fail = (M) x (C) = $4.2(10^{-4}) \times 6.1(10^{-4})$

= $2.6(10^{-7})$

Which is << than 10^{-5} **RESULT!!**



NO MORE MATHS……..

Lessons Learnt

- Functionality and Operational Realities are Critical – Talk to the Pilot.
- Consider the integrated system functionality at an aircraft level.
- Functional testing alone does not deliver 1309 compliance; only checks behaviour when systems are working properly. System must be designed to FAIL WELL as much as WORK WELL.
- "Non-Essential" systems can lead to hazardous/catastrophic failure of "Essential Systems" by transfer of failures across interfaces.
- Systems overlap i.e. electrical control panel for 'top-up' tanks effecting the aircraft primary fuel system safety.
- Calculating reliability of a complex assembly of components is tedious – simplified parts count approach is a quick/conservative approximation.
- Never believe anyone who says "*it's just a non-essential system*".

QUESTIONS?