

***Functional Hazard Analysis
What?
The Why & How (RNZAF style)***



FLTLT Darryn Welham

Technical Services Aeronautical Software

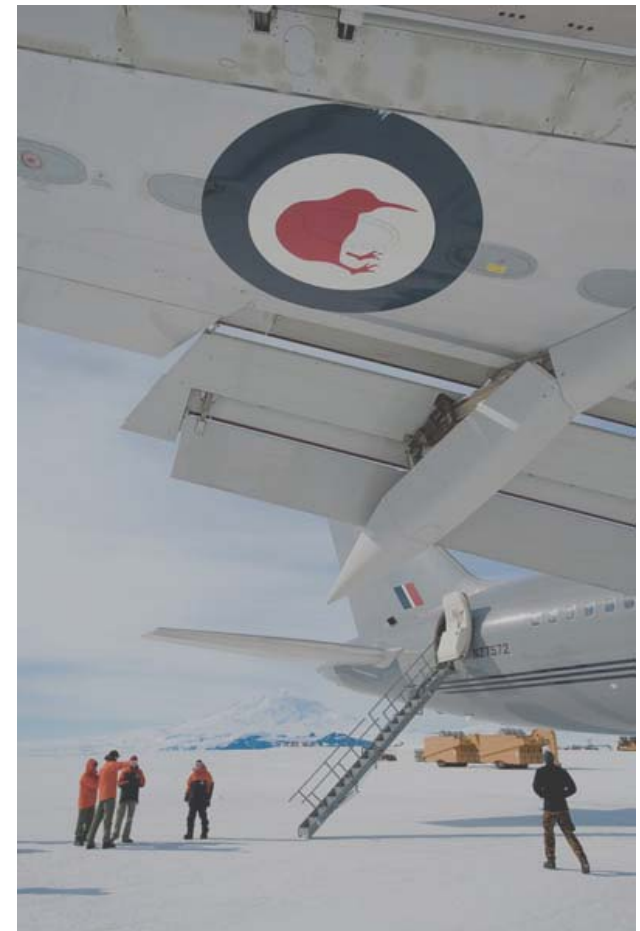
Functional Hazard Analysis

- What?
- Why?
- How?



My Background

- Staff Officer in the RNZAF Technical Services Aeronautical Software



References

- FAA 2x.1309
- SAE/ARP 4761
 - Guidelines and Methods for Conducting the Safety Assessment on Civil Airborne Systems and Equipment
- SAE/ARP 4754
 - Certification Considerations for Highly-Integrated or Complex Aircraft Systems
- NZAP 6000
 - Technical Airworthiness Manual, Leaflet D7.1
- AAP 7001.054 (AM1)
 - Airworthiness Design Requirements Manual

What?

- FHA
- Clue is in the name
- Part of a System Safety Plan



Why?

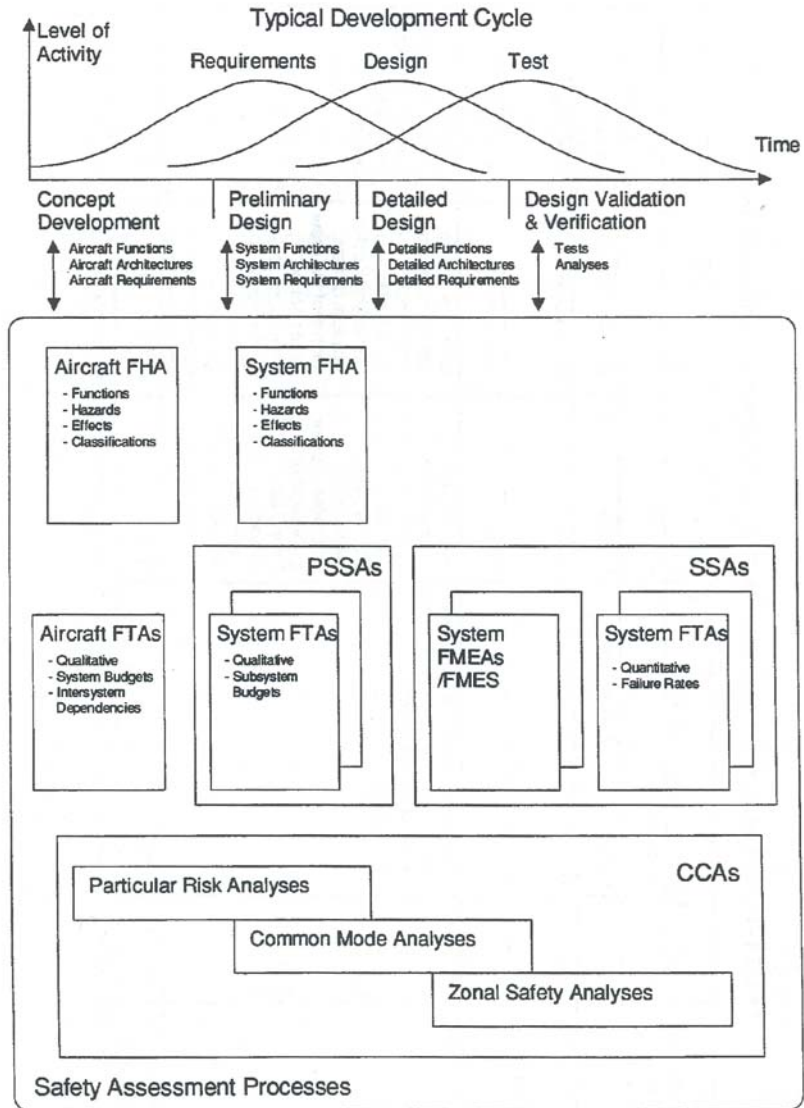
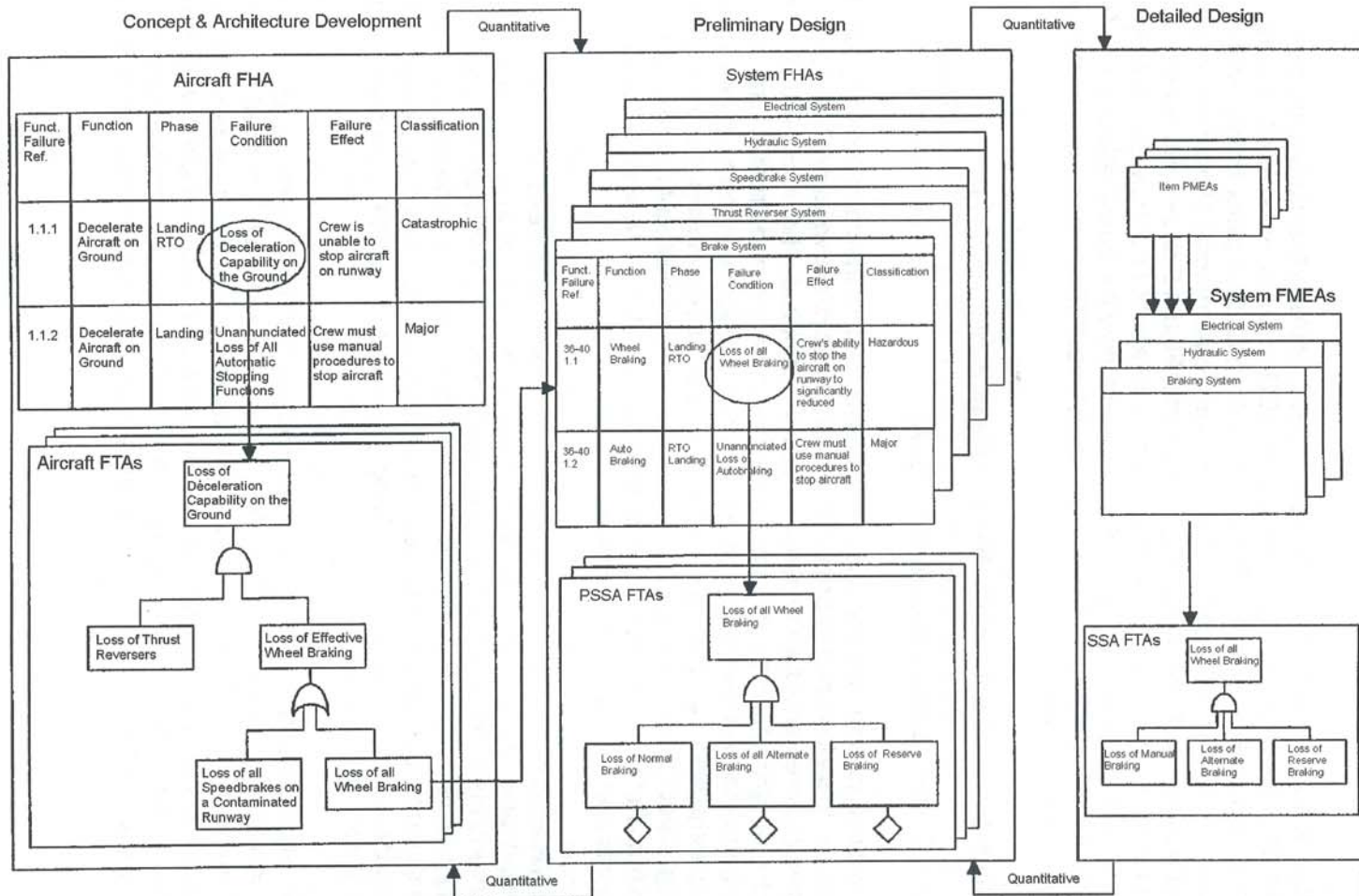


FIGURE 1 - Overview of the Safety Assessment Process

Why?

FIGURE 2 - Example of the Relationship Between FHAs and FTA/FMEAs



Why?

- The RNZAF Perspective
- Needs to be simple, cheap and effective
- It is RNZAF policy that appropriate FHAs, or similar safety assessments are to be conducted on all NZDF aircraft and aeronautical equipment configuration changes.

How

According to the SAE ARP4761

- May be Aircraft Level or System Level functions
- Qualitative Assessment which is iterative
- Top down approach

How

According to the SAE ARP4761

- Identify all the Functions a system (or aircraft) has,
- Identify & Describe Failure Conditions,
- Determine the Effects of the Failure Condition,
- Classification of Failure Condition Effects,
- Assignment of requirements to lower levels
- Identification of supporting material
- Identification of method to verify compliance

How

According to RNZAF TS Aero Soft

- Simply systematically identify:
 - the functions a system (or aircraft) has,
 - consider how they fail,
 - what impact that failure will have,
 - any mitigation or backups, and
 - the resultant hazard classification.

How

- The NZAP:

NZAP 6000 Part
Leaflet D7.1 Functional Hazard Analysis/System Safety Assessment

AL 10
01 April 2011

- 1.8 The FHA should be conducted using the procedure and annexes contained in NZAP 6004-1, [Leaflet C7](#). Assessments are to be independently reviewed and checked by a suitably experienced person for endorsement before being added to the configuration change certification package.
- 1.9 At least two persons are to conduct the FHA to ensure robustness of assessment depth through diversity of perspective. While each person may fulfil more than one role, the FHA should be conducted by a team comprising appropriate user(s), maintainer(s), design Subject Matter Experts (SME), engineer(s) and a recorder, and be led by a suitably experienced person.
- 1.10 The completed FHA is to contain a summary which discusses the occurrence and acceptability of all hazards identified in the FHA report as being major or above in accordance with the Hazard Classifications tabled at NZAP 6004-1, [Leaflet C7](#), Annex B. Should impact to mission need to also be considered, the definitions of NZAP 6004-1, [Leaflet C7](#) Annex C (and AAP 7001.054, Section 2, Chapter 7 for software) can be used as a guide.
- 1.11 All hazards identified by the FHA process that are assessed as Major or above are to be designed such that their chance of occurring are in accordance with the probability table in NZAP 6004-1, [Leaflet C7](#), Annex B. Assurance of this in a quantitative manner by Fault Tree Analysis or Failure Modes and Effects Analysis, or similar is to be provided in the configuration change development report. Exception may be made where the design is simple and conventional or redundant.
- 1.12 The FHA is separate to but interrelates with the airworthiness secretariat ACMB Platform Risk Register. Hazards identified by the FHA that are not able to be mitigated or designed to the required probability of failure margins will either prevent the incorporation of the proposed system or need to be accepted by the Technical Airworthiness Authority (TAA) and Operating Airworthiness Authority (OAA) and transferred to the Platform Risk Register.

How

- The NZAP:
 - Form a group of SMEs
 - Run through the template
 - Write it up in a summary Report
 - Get independent review

How

- The RNZAF template

System	Reference No.	For reference during the assessment		
	System	The system modification is to.		
	Sub-system	Subsystems that make up part of the modified system. May be multiple.		
	Function	Consider the functions of each subsystem. May be Multiple		
Hazard Considerations	Malfunction	Consider how the (sub) system may malfunction. E.g. not function when demanded, function when not demanded, function incorrectly		
	Environment	Consider e.g. drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, radiation - including laser...		
	Impact on Aircraft	What effect would this have on the performance and structure of the aircraft?		
	Impact on Crew	Would this be hazardous/fatal to crew? Would this increase crew workload?		
	Impact on Other Personnel	Would this be hazardous/ fatal to other personnel, (e.g. passengers or maintainers)? Would this increase maintainers or others workload?		
	Impact on Other Systems	For the specified system/subsystem, consider its interactions with other systems and what impact its failure would have on those.		
	Hazard Severity	Catastrophic, Hazardous, Major, Minor, No Effect (see NZAP 6000 Leaflet ?? for definitions)		
	Previous Problems and their Impact	Any historical issues, in-service use, faults of the past Did they affect flight mission, how?		
Mitigation	Backup Systems	Is there a backup system?		
	Impact of back-up System	Does using BU system have adverse affect on a/c, crew, passenger, safety or pilot workload?		
	Risk of Failure of Backup	What is the likelihood of the BU to fail? If BU was to cease functioning haz/fat to a/c or crew? How would a/c / crew be affected by BU system not functioning?		
	Other Mitigation	Any other mitigation strategies? E.g. Training or Procedures		
	Resulting Hazard Severity (post mitigation)	Catastrophic, Hazardous, Major, Minor, No Effect (see NZAP 6000 Leaflet ?? for definitions)		
Conclusion	Required Probability to Better	Extremely Improbable, Extremely Remote, Improbable, Probable, No Requirement, (or for software -the Assurance Level)		
	Actual Developed Reliability			
	Gap			

Example

- The Moving Map Device with USB GPS Antenna

Reference No.	For reference during the assessment	1.1	1.2	1.2
References	Documents referenced:	40 SQN SOP's : \\SWHERES9\Public\public\1\Education\Publications\library\OpsPubsforSharePoint\SOP_C130_AL14.pdf PAN Risk register: http://org/air-dlog/DAEAirworthinessDocuments/restricted%20PAN%20Risk%20Register.xls		
System	The system modification is to.	<p>Moving Map Software:</p> <p>Falconview moving map software is [to be] installed on the aircrafts existing moving map laptop located on the C-130 at the navigator station.</p> <p>Falconview is "a multi-media mapping package for the PC that displays various types of maps and geo-referenced overlays". Overlays include: Manoeuvre Graphics, Enemy threats, maps, basic shape overlays, imagery, digital map data, elevation data. Falconview supports many other functions and features including: Co-ordinate conversion, ability to manage maps and World Vector Shoreline information, Support for DIFAF and NAVPLAN, NAVPLAN databases, Ground Route Planning, ICAO airfield information, calculation of time and distance travelled, fuel usage, display of rasterized data (CADRG, ONC, Jetnav) etc.</p>		
Sub-system	Subsystems that make up part of the modified system. May be multiple.	Displayed information (Static)	Displayed information (moving)	
Function	Consider the functions of each subsystem. May be Multiple	Static information including: Maps Terrain Features, airspace, no fly zones,	Own Ship Location: Historical Position	Own Ship Location: Current Position
Stated Usage	Stated use for displayed data.	To provide the navigator with pictorial representation of important features in the area of operation, to add to the 'situational awareness' of the navigator, as part of their standard scan (per C-130 SOP's)	To provide the navigator with a history of where the aircraft has been, to achieve the reporting requirements of 40 SQN SOP's.	To provide the navigator with a graphical representation of the current location of the aircraft in relation to the displayed static features, to aid in decision making. Used in conjunction with other navigation systems as 'Situational Awareness'.
Description	Description of displayed data	Static images of map features	Digital icon 'breadcrumbs' showing previous aircraft position. Items laid at intervals.	Aircraft ownship (crosshair) in relation to terrain features displayed on pictorial map and in relation to other overlays.

Mitigation	Is this the primary Source?		No. Standard aircraft Instrumentation and navigation sources provide the primary information.	No. Standard aircraft Instrumentation and navigation sources provide the primary information.	May be primary source of track history	Standard aircraft navigation sources provide the primary information.
	Backup Systems	Is there a backup system when this system fails.	Visual navigation using waypoints referenced off the aircraft GPS and INS is the primary method. MMD secondary reference.	Visual navigation using waypoints referenced off the aircraft GPS and INS is the primary method. MMD secondary reference.	manual plotting, however, not currently required by 40 SQN SOP's when moving map fitted.	primary method
	Impact of back-up System	Does using BU system have adverse affect on a/c, crew, passenger, safety or pilot workload?	Slight increased in workload through manual plotting	If primary methods of navigation are not available, Falconview may inadvertently become the primary reference.	Increased workload through manual plotting	Increased workload
	Risk of Failure of Backup	What is the likelihood of the BU to fail? If BU was to cease functioning haz/fat to a/c or crew? How would a/c / crew be affected by BU system not functioning?	Primary source (INS) failing may result in use of Moving Map as Primary	Primary source (INS) failing may result in use of Moving Map as Primary	Unlikely (manual system)	Unlikely
	Other Mitigation	Any other mitigation strategies? E.g. Training or Procedures	Not clear on training and crew knowledge of limitations of Falconview. Not recorded in the flight manual or SOP's. Collision avoidance systems, Radar altimeter, countermeasures.	Requires Training and SOP's to mitigate the above risks: Not to be used for terrain avoidance Not to be used in IMC Not to be used for separation from restricted airspace. Radar altimeter provides some mitigation, however attempts to correlate to moving map altitude may be difficult in undulating terrain.	Nil.	Nil
	Resulting Hazard Severity (post mitigation)	Catastrophic Hazardous, Major, Minor, No Effect <i>(see NZAP 6002-10 for definitions)</i>	loss of display would result in Minor failure condition through slight increase in crew workload and slight reduction in safety margins	With mitigations in place, incorrect map projection would result in Minor failure condition related to only minor increase in workload.	Incorrect map projection would result in Minor failure condition due to incorrect information being provided post-flight	loss of display would result in a Major failure condition through slight increase in workload and slight reduction in safety margins
Conclusion	Required Probability	Extremely Improbable, Extremely	Level D	Level D	Level D	
	Actual Developed Reliability	Level E, no assurance measures.				
	Gap		1 steps +	1 steps +	1 steps +	
Summary of Mitigation Factors, to be taken to SOPs or Hazard Log	Capture all Mitigation Factors leading to Safety Level Include Action Item e.g. "Warning to be incorporated...."	Note for flight manual / SOP's or temporary order: Limitations with incorrect map projections in Falconview may occur. Data may not be correct. Use primary sources of navigation information.	Requires documenting approved uses to mitigate the above risks: Not to be used for terrain avoidance Not to be used in IMC Not to be used for separation from restricted airspace.			

ons	Malfunction	Consider how the (sub) system may malfunction. E.g. not function when demanded, function when not demanded, function incorrectly	Fails to display static features (blank screen, or obvious error).	Displays hazardous misleading information related to static features (i.e. undetected erroneous data such as system lat/long over geographical point not matching real world)	Fails to display, or displays actual Lat/Long over incorrect map projection.	Fails to display location failure or software
	Environment	Consider e.g. drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire,	N/A (Software)	N/A (Software)	N/A (Software)	N/A (Software)
	Impact on Aircraft	What effect would this have on the performance and structure of the aircraft?	Crew resort to normal procedures (non-moving map procedures)	Hazardous Misleading information may affect crew decision making causing: + undetected map projection may cause unintended incursion into restricted airspace, + undetected incorrect Elevation data in IMC may lead to collision with terrain. + undetected map projection in IMC, accompanied with use of correct elevation data may lead to collision with terrain.	Undetected map projection may lead to incorrect information provided during post-flight analysis and may result in false intel provided to supporting units.	Crew resort to normal procedures (non-moving map procedures)
	Impact on Crew	Would this be hazardous/fatal to crew? Would this increase crew workload?	Slight increase in workload.	Recovery from incorrect decision making (once realised) could exceed crew workload, or could result in Catastrophic (CFIT), or incursion into restricted airspace (enemy /politically sensitive)	May result in increased risk to coalition forces.	Slight increase in workload manual / traditional methods
	Impact on Other Personnel	Would this be hazardous/ fatal to other personnel, (e.g. passengers or maintainers)? Would this increase maintainers or others workload?	nil	nil	nil	nil
	Impact on Other Systems	For the specified system/subsystem, consider its interactions with other systems and what impact its failure would have on those.	nil	nil	nil	nil
	Hazard Severity	Catastrophic Hazardous, Major, Minor, No Effect (see NZAP 6002-10 definitions)	Minor / No Effect (slight increase in crew workload)	Catastrophic / Hazardous	Minor / No Effect (slight increase in crew workload)	Minor / No Effect (slight increase in crew workload)
	Previous Problems and their Impact	Any historical issues, in-service use, faults of the past Did they affect flight mission, how?	Known issues with mapping projection in Falconview. Known problems relating to assurance of data (see ACMB risk register)	Known issues with mapping projection in Falconview. Known problems relating to assurance of data (see ACMB risk register)	Known issues with mapping projection in Falconview. Known problems relating to assurance of data (see ACMB risk register)	Nil

Reference No.	For reference during the assessment		1.3	1.4	1.5
References	Documents referenced:				
System	The system modification is to.		Globalsat BU-353 USB GPS Receiver		
Sub-system	Subsystems that make up part of the modified system. May be multiple.		GPS Receiver	Window suction cup bracket for GPS receiver	
Function	Consider the functions of each subsystem. May be Multiple		Provides C/A GPS signal to moving map over USB.	Holds GPS receiver to get signal	
Stated Usage	Stated use for displayed data.		To provide position update to PFPS	N/A	
Description	Description of displayed data		Aircraft ownship (crosshair) in relation to terrain features displayed on pictorial map and in relation to other overlays.		

Hazard Considerations	Malfunction	Consider how the (sub) system may malfunction. E.g. not function when demanded, function when not demanded, function incorrectly	Degraded signal, (either by not responding fast enough, not enough satellites, not taking into account vertical gain, no military code...)	Falls off; falls off in crash/aggressive flying - hits/jams controls or switches; Bracket wears out	Damage to window, applies extra stresses in addition to max PD during 3G manoeuvre exceeding structural limits of window.
	Environment	Consider e.g. drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire.	Multiple parts of globe; not optimum position on aircraft; Internal antenna.	vibration, G forces	Dust, rain, wind, temperature and pressure differential, high G manoeuvre (worst case)
	Impact on Aircraft	What effect would this have on the performance and structure of the aircraft?	Undetected degraded signal, contributes to possibility of misleading information, could result in emergency terrain avoidance or infringing on unfriendly airspace, worst case loss of airframe.	If turns off then fine, can use back-up. But if hits controls or switches could break some of aircraft. Can be partially mitigated through use of tiewraps onto nearby structure	Structure of aircraft degraded. Weight of GPS may contribute to window breaking at altitude (max PD), conditions increased if conducting emergency manoeuvre (avoidance / countermeasure)
	Impact on Crew	Would this be hazardous/fatal to crew? Would this increase crew workload?	Recovery from incorrect decision making (once realised) could significantly increase, worst case could result in Catastrophic (CFIT). Possible incursion into restricted airspace (enemy /politically sensitive)	If turns off then fine, can use back-up. But if hits controls or switches would increase crew workload – however easily mitigated.	Potential decompression situation, emergency oxygen use required at altitude. Significant increase in crew workload.
	Impact on Other Personnel	Would this be hazardous/ fatal to other personnel, (e.g. passengers or maintainers)? Would this increase maintainers or others workload?	as above	as above	Potential hypoxia situation for passengers. Increased workload for maintenance & support staff
	Impact on Other Systems	For the specified system/subsystem, consider its interactions with other systems and what impact its failure would have on those.	as above	as above	-
	Hazard Severity	Catastrophic Hazardous, Major, Minor, No Effect (see NZAP 6002-10 definitions)	Catastrophic / Hazardous	Minor	Hazardous
	Previous Problems and their Impact	Any historical issues, in-service use, faults of the past Did they affect flight mission, how?	Does not provide military accuracy; Non-real-time update on Laptop. Subject to Jamming / Spoofing (no RAIM).	unknown	unknown

Mitigation	Is this the primary Source?			N/A
	Backup Systems	Internal aircraft GPS, manual plotting.MMD is secondary reference.	No	No
	Impact of back-up System	Increased workload through manual plotting	Increased workload through manual plotting	-
	Risk of Failure of Backup	Primary source (INS) failing may result in use of Moving Map as Primary.	-	-
	Other Mitigation	Procedures could be made/used to ensure the likely inaccuracy of the system is accounted for. (i.e. 1NM range ring around A/C to highlight system potential) Radar altimeter, provides some mitigation against encroaching terrain, countermeasures provide some mitigation of enemy airspace incursion.	Put where not going to fall on anything important.	Be gentle with it, don't remove replace frequently, as this also adds to the chance of failure. Mitigation for loose article risk requires stowing at take-off/ landing. Must be within the crews capacity to remove and stow during take-off, landing, turbulence emergency conditions; OR have antenna correctly mounted on mount approved by structures officer.
	Resulting Hazard Severity (post mitigation)	loss of display of aircraft position would result in a Minor failure condition through slight increase in crew workload and slight reduction in safety margins	loss of display of aircraft position would result in a Minor failure condition through slight increase in crew workload and slight reduction in safety margins	If mount is not approved by structures officer: Major , significant increase in workload/impairing crew efficiency. If mount is approved by structures officer: No effect
Conclusion	Required Probability	Minor failure may be Probable, 10E-5	Minor failure may be Probable, 10E-5 to	Major failure must be Improbable, 10E-5<
	Actual Developed Reliability	No data available, therefore assumed to be likely 10E-3	No data available, therefore assumed to be likely 10E-3	
	Gap	1 steps +	1 Step +	
Summary of Mitigation Factors, to be taken to SOPs or Hazard Log				Mount to be approved by structures officer.



Summary

- FHA is initial cut, feeds into rest of SSA
- Complete (RNZAF style) by systematically identify:
 - the functions a system (or aircraft) has,
 - consider how they fail,
 - what impact that will have,
 - any mitigation or backups, and
 - the resultant hazard classification.
- Excel template available from FLTLT Darryn Welham
darryn.welham@nzdf.mil.nz

Questions???

