Annex D Safety Assessments

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Union Aviation Safety Agency (EASA). Neither the European Union nor EASA can be held responsible for them.

CONTRACT NUMBER:	EASA.2020.C02
CONTRACTOR / AUTHOR:	DART Aerospace
IPR OWNER:	European Union Aviation Safety Agency
DISTRIBUTION:	Public

APPROVED BY:	AUTHOR	REVIEWER	MANAGING DEPARTMENT
D. Shepherd	G. Karvonen	A. Flores M.L. Scatola M. Selier	DART Engineering

DATE: 26 February 2024

CONTENTS

1. Functional Hazard Assessment

Item No.	Function	Critical Function (Y/N)	Failure Condition Hazard Description	Phase of Flight	Effect of Failure Condition on Aircraft/Crew	Classification of Failure Condition		Analysis Considerations and Remarks
						Total Loss of Function	Partial Loss of Function	
1	**HEFS SYSTEM FUNCTIONS**							
1.1	Inflate HEFS when required	Y	Failure to inflate the HEFS floats when required	Post ditching/ survivable water impact	Failure to inflate when required can result in insufficient air pocket in the rotorcraft and insufficient air pocket generated in the rotorcraft. No possible crew actions.	Hazardous (fail to inflate when required)	Minor (Assumes functional sensor path to HEFS relay remains operational and sufficient air pocket is created)	Failure to inflate either float will result in insufficient air pocket inside the rotorcraft once capsized. Only one compartment is allowed fail to to inflate. Could result in serious or fatal injury to a passenger or crew member.
1.2	Prevent HEFS activation when not commanded	Y	Inadvertent activation	All (Engines ON) and auto-rotation	Activation of the HEFS can cause damage to main rotor if activated in flight. High risk of entanglement is considered. No possible crew actions.	Catastrophic (either side inflating when rotors moving)	Major (failure of partial activation path ON, or safety system being ineffective, resulting in significant reduction in safety margin)	Either float inflating during flight has a chance to damage or entangle the main rotor blades, possibly resulting in a catastrophic failure.
1.3	Prevent HEFS activation when not commanded	Y	Inadvertent activation	Ground (Engines OFF)	Tested in pre-flight check with engines OFF and crew away from floats, no safety risk.	NSE	NSE	No safety risk to crew or ground personnel.

Table 1 Functional Hazard Assessment

2. Fault Tree Analyses

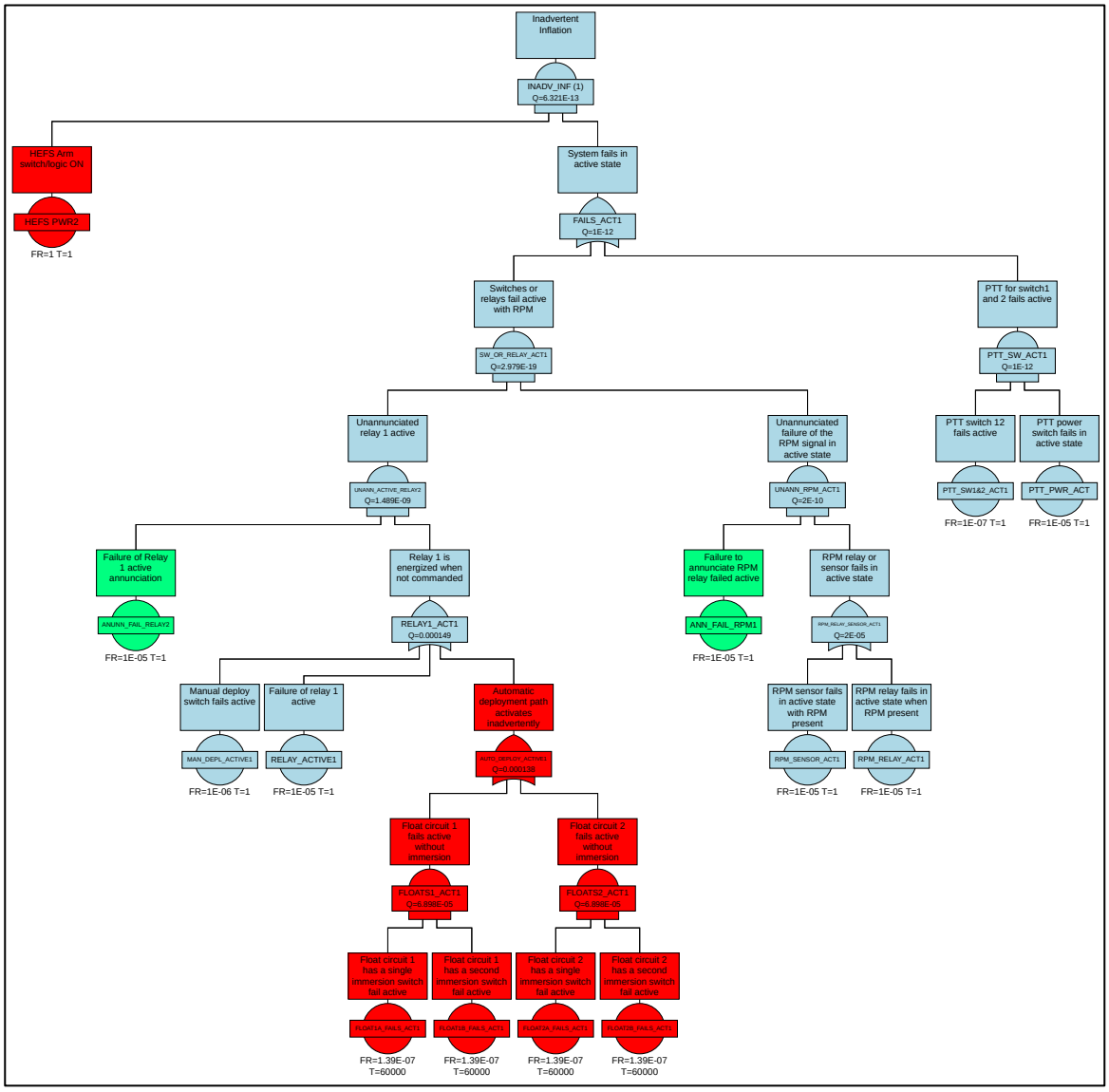

Figure 1 Fault Tree Analysis inadvertent deployment

The red items in the figure above are items already present in the helicopter. The green items are annunciators. The other items are the HEFS hardware components.

The top-level safety objectives for the design were 10E-9 per flight hour for inadvertent inflation, and 10E-7 per flight hour for failure to deploy when required.

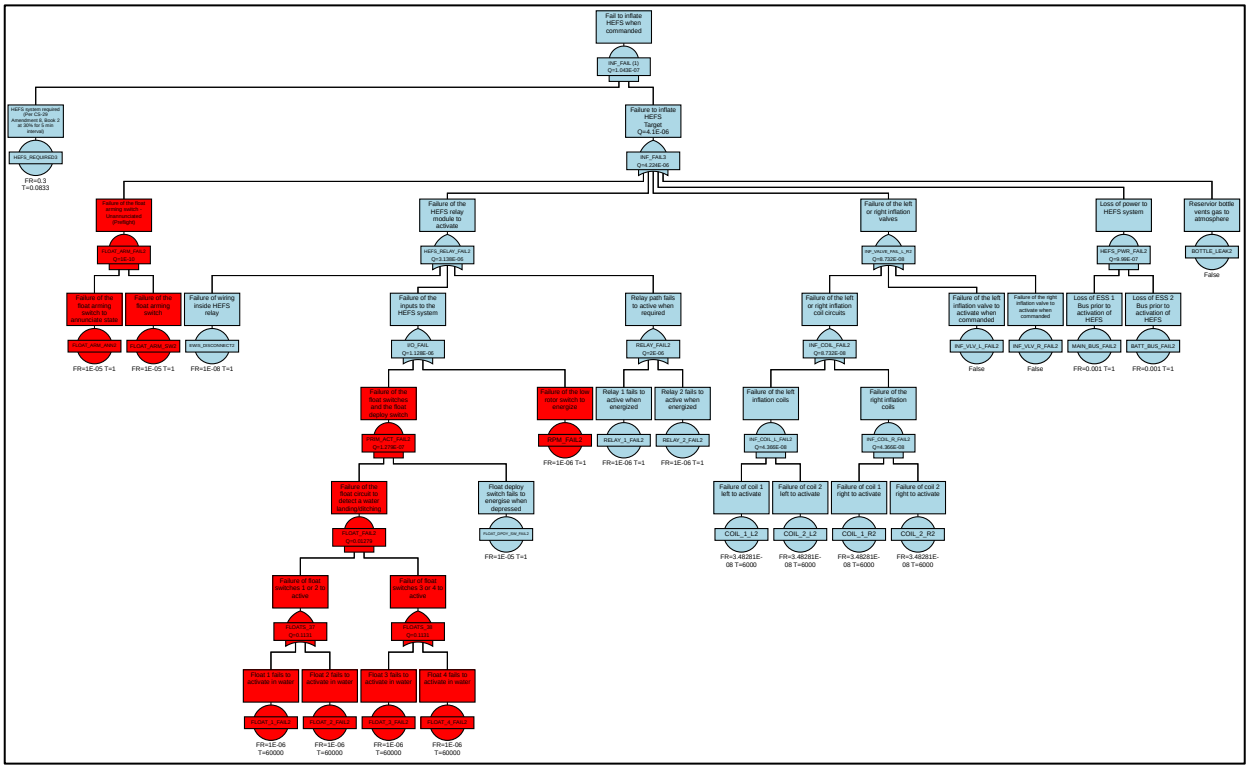

Figure 2 Fault Tree Analysis failure to deploy

3. Failure Modes and Effects Analysis

Note: this FMEA was executed on the HEFS design considered for this EASA research project on offshore operations and High Emergency Flotation System. For other system designs, the FMEA may be different.

#	Component	Function	Mission Phase	Failure Mode	Detection Means	Failure Description	Failure Effects
1	Float Arming Switch/logic	Provide power to float systems	All	Fails ON	Illuminated switch. Preflight check to be performed.	Switch fails in the ON position power is continuously fed to the system	Power provided to the system does not present a risk during flight but reduces the safety margin wrt inadvertent inflation.
			All	Fails OFF	Switch does not illuminate, pilot preflight check.	EFS systems will not be able to arm (not available)	EFS not available. If system not available, crew to refer to MMEL.
2	Float Deployment Switch	initiate float deployment	Ground	Fails ON	Annunciated on switch. Periodic inspection of system required.	Deployment switch is stuck ON	When floats are ARMED (Probability of 1) and the deployments switch fails ON, system is controlled by the RPM sensors, which will not allow inflation if RPM is present. Failure will annunciate to crew and allow time for corrective action if required.
			Ditching	Fails OFF	None. Latent until activation.	Deployment switch fails to trigger float activation	EFS and HEFS still have the automatic activation path
3	Float Immersion Switch	Provides power to RPM sensor path when submersed.	All	Fails ON	None. Potential latent failure.	Remaining float switch in series will be relied on for activation	Reduced safety margins for inadvertent float activation

#	Component	Function	Mission Phase	Failure Mode	Detection Means	Failure Description	Failure Effects
			Ditching	Fails OFF	None. Potential latent failure.	Single switch failure will result in one of the two float switch loops becoming inactive.	One of two loops still functional, additional activation means through float deployment switch
7	Lower Rotor RPM Sensor		Ditching	Fails ON (RPM is active)	Primary low rotor speed detection shows RPM is present. Indicated to crew is assumed from existing rotorcraft systems.	RPM active will not allow activation signal path to HEFS Relay	HEFS will not be allowed to activate when command
			Ditching	Fails OFF (RPM is not active – Low RPM)	None. Potential latent failure.	HEFS system will only rely on float sensors to activate or manual activation switch	HEFS has reduced safety margins and will rely on the float sensors or deployment switch
8	Reserved						
	Reserved						
9	HEFS Relay	HEFS activation command to valves	All	Fails active	BIT function, annunciated to crew.	HEFS relay remains in the active position (energized) when HEFS not armed	Cannot disarm HEFS system
		HEFS activation command to valves	Ditching	Fails OFF	BIT function, annunciated to crew.	HEFS relay will fail to activate when commanded.	HEFS system unavailable
10	LH Inflation Valve Coil 1 or 2	Activate gas release to floats	Ditching	Fails to activate when commanded	None. Potential latent failure. Overhaul period to be required.	One of two coils fails to fire	Failure of a single coil will still result in valve activation
11	RH Inflation Valve Coil 1 or 2	Activate gas release to floats	Ditching	Fails to activate when commanded	None. Potential latent failure. Overhaul period to be required.	One of two coils fails to fire	Failure of a single coil will still result in valve activation

#	Component	Function	Mission Phase	Failure Mode	Detection Means	Failure Description	Failure Effects
12	LH or RH Valve Internal Firing Mechanism	Release high pressure gas when activated	Ditching	Fails to activate when commanded	None. Potential latent failure. Overhaul period to be required.	Mechanism will not rupture disk and release gas.	Single side failure will still result in partial inflation of both floats, assummed to provide an air pocket.
13	LH or RH Gas Cylinder	Contain high pressure gas	Ditching	Cylinder Leaks	Cylinder pressure checked preflight.	May result in insufficient pressure available	Single side failure will still result in partial inflation of both floats, assummed to provide an air pocket.
14	LH or RH Inflation Hoses	Distribute gas to floats	Ditching	Hose disconnects	None. Hoses properly qualified for application and proof tested. Periodic inspection required.	Hose failure does not allow gas to float.	Single side failure will still result in partial inflation of both floats, assummed to provide an air pocket.
		Distribute gas to floats	Ditching	Hose Leaks	None. Hoses properly qualified for application and proof tested. Periodic inspection required.	Small leaks will likely still result in float inflation. Large leaks are the same as a hose disconnect.	Single side failure will still result in partial inflation of both floats, assummed to provide an air pocket.
15	LH or RH Float	Provide buoyancy	Ditching	Single Compartment Leak	Latent until inflation	Not all compartments inflate.	Only one compartment is allowed to fail to inflate in order to still achieve the required air pocket
		Provide buoyancy	Ditching	Complete containment failure	Latent until inflation.	Float fails.	Insufficient floats to achieve air pocket

Table 2 Failure Modes and Effects Analysis

4. Common Mode Analysis

The AND gates from the fault tree analysis are listed in Table 3. Each of these gates are assessed to ensure there is nothing that invalidates the assumptions of independence.

Fault Tree	AND Gate	Analysis Considerations
Inadvertent Inflation	INADV_INF (1)	HEFS PWR2 is a requirement for the system to be powered that cannot fail in a way that would result in the inadvertent activation of the system
	SW_OR_RELAY_ACT1	The two relay paths need to be electrically isolated so no failure mode can cause the other relay to fail active. Single relay active failures are annunciated to the crew. [SR]
	PTT_SW_ACT1	For this circuit to fail active, the PTT power switch would have to fail in a manner that provides power to the relay switch AND the ARMed circuit. Additionally, the PTT switch for each relay would need to fail in a manner that passes power to both sides of the switch. Each failure mode is independent. [SR]
	UNANN_ACTIVE_RELAY2	The sensor relay needs to fail active AND the annunciation of this state would need to fail inactive. Note that if the sensor relay fails active on the ground with no RPM, the system can activate. If RPM is present, this failure cannot activate the system.
	FLOATS1_ACT1	Float circuit 1 consists of 2 float switches in series. The circuit cannot activate without both floats being activated by water entering the float. No common mode failures exist. [SR]
	FLOATS2_ACT1	Float circuit 2 consists of 2 float switches in series. The circuit cannot activate without both floats being activated by water entering the float. No common mode failures exist. [SR]
	UNANN_RPM_ACT1	The RPM relay needs to fail active AND the annunciation of this state would need to fail inactive. The RPM signal by itself cannot activate the system without the sensor inputs active or the manual deployment switch active. [SR]

Fail to inflate HEFS when required	INF_FAIL (1)	The HEFS is ANDed with the probability that the HEFS is required due to potential capsize. The HEFS reliability is independent of this probability.
	FLOAT_ARM_FAIL2	The float arming switch would need to fail and the annunciation would not reflect the current state. The annunciation and the arming switch would need to maintain independence. [SR]
	PRIM_ACT_FAIL2	Failure of the float switch circuits and the manual deploy switch to activate the HEFS when commanded. Both circuits are independent. [SR]
	FLOAT_FAIL2	Failure to activate float circuit 1 and 2 in the event of a water landing. Dual float circuits are required with 2 switches per circuit. [SR]
	INF_COIL_L_FAIL2	Failure of inflation valve 1 of both coils. Either coil activating will activate the system. No common mode failures can exist for the coils, which are simple electrical devices. [SR]
	INF_COIL_R_FAIL2	Failure of inflation valve 2 of both coils. Either coil activating will activate the system. No common mode failures can exist for the coils, which are simple electrical devices. [SR]
	HEFS_PWR_FAIL2	Power for the HEFS is supplied by 2 ESS busses. These power sources are already considered reliable and independent due to the current ditching requirements for the rotorcraft. Power for the HEFS must be provided by 2 sources per the design schematic. [SR]

Table 3 Common Mode Analysis

European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3
50668 Cologne
Germany

Mail EASA.research@easa.europa.eu
Web www.easa.europa.eu

An Agency of the European Union