AtkinsRéalis

Hazard Identification

Plan Design Enable

AtkinsRéalis

Learning Objectives

- Objective:
  - To understand why and when Hazard Identification is needed in accordance with Aerospace Recommended Practice (ARP) 4761 and MAA Guidance
  - To appreciate the different techniques available and used within the ARP
- Topics to be Covered:
  - What is a Hazard?
  - Why Hazards should be identified?
  - Methods of Hazard identification.

What is a Hazard?

- "A physical situation or state of a system, often following some initiating event, that may lead to an accident." *[Def STAN 00-056]*
- "An intermediate state where potential for harm exists" *[MAA02, ASPIRE 17.A.1.i]*
- "A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof" *[ARP 4761].*

Accident Sequence

Initiating Event(s) → Hazardous State → Accident

Hazardous to Whom or What?

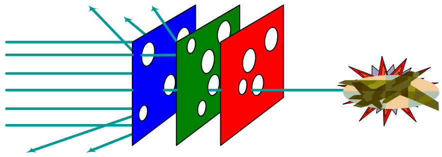
- Operators
- Users

- Maintainers
- Passengers
- Members of the Public, 3rd Parties

Why Identify Hazards?

- **To try and prevent accidents!**

- Equipment providers (DE&S) manage safety by managing hazards
  - Elimination / Control / Mitigation

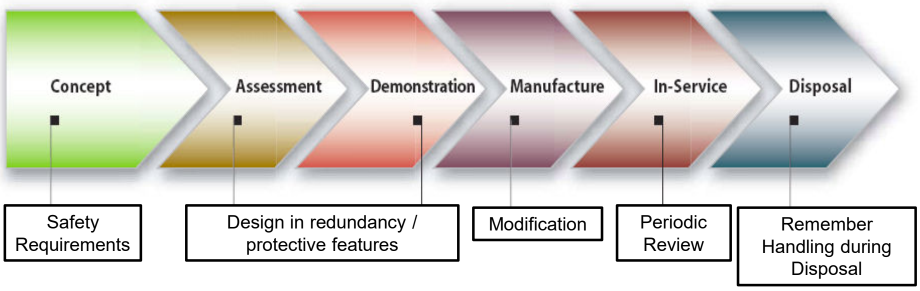


- Priority of risk reduction
  - Removal of the hazard
  - Substitution of hazard (by use of alternative substances / procedures)
  - Passive physical controls (fail safe)
  - Active physical controls (activation of interlocks)
  - Personal Protective Equipment (PPE)
  - Provision of safety procedures, warnings, training, etc.

- **Strive to identify ALL hazards and record them.**

When to Identify Hazards?

- In time for the results to be useful!



AtkinsRéalis

Hazard Identification Methods

- Generic term when carrying out Hazard Identification is **HAZID**
- There are a number of well developed and established techniques:
  - Past Experience
  - Standards and Regulations
  - Brainstorming
  - Checklists
  - Structured What If Technique (SWIFT)
  - Hazard Operability Study (HAZOP)
  - Functional Hazard Assessment (FHA)
  - Failure Modes and Effects Analysis (FMEA)
  - Failure Modes Effects and Criticality Analysis (FMECA)
  - Zonal Hazard Analysis (ZHA)
  - Particular Risk Analysis (PRA)
  - and many more…..

AtkinsRéalis

Structured What-If Technique (SWIFT)

- SWIFT is a **holistic** assessment of a system using a structured "brainstorming" method where "What If" questions are generated from a number of sources:
  - Checklists
  - Standards, regulations & guidelines
  - Past incidents and accidents.

Project: Aircraft Fuel System					**Page No**	
Description: The fuel tank, engine inlet/outlet pipes and hoses, fuel pump, fuel filter						
Ref	**Question Category**	**What If**	**Cause/ Failure**	**Consequences**	**Safeguards**	**Recommendations**
1						
2						
3						

AtkinsRéalis

Structured What-If Technique (SWIFT)

- SWIFT is a **holistic** assessment of a system using a structured "brainstorming" method where "What If" questions are generated from a number of sources:
  - Checklists
  - Standards, regulations & guidelines
  - Past incidents and accidents.

Project: Aircraft Fuel System					Page No	
Description: The fuel tank, engine inlet/outlet pipes and hoses, fuel pump, fuel filter						
Ref	Question Category	What If	Cause/ Failure	Consequences	Safeguards	Recommendations
1	Material properties	Fuel leaks	Chafing of hose	Fire	Drain holes	Fire suppression
2	Material properties	No fuel	Pump failure	Engine Stops	Warning Light	
3	Instrumentation	Erroneous fuel level reading	Sticking gauge	Run out of fuel – engine stops	Servicing	Secondary sensor

AtkinsRéalis

Hazard Operability Study (HAZOP)

- **Systematic** examination of the system design for **deviations from the design intent** leading to Hazards or Operability Problems
  - Follows structured guide words for completeness.

Project: Aircraft Fuel System				Page No	
Description: The fuel tank, engine inlet/outlet pipes and hoses, fuel pump, fuel filter					
Ref	Guideword	Causes	Consequences	Safeguards	Recommendations
1	More Pressure				
2	Less Pressure				
3	Reverse Pressure				

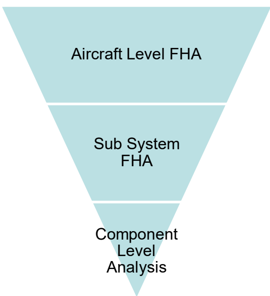
Functional Hazard Assessment (FHA)

- **Systematic** high level examination of a **functional representation** of the system to determine effects from the following failure modes categories:
  - Loss of function
  - Function provided when not required
  - Incorrect operation of function.

Project: Engine System				Page No		
Description: The Engine, air system, fuel system, lubricating system, exhaust system, cooling system						
Ref	**Function**	**Failure Condition**	**Phase**	**Effects**	**Safeguards**	**Recommendations**
1	To provide thrust					
2	To drive a shaft (generate electricity)					
3	To provide bleed air					

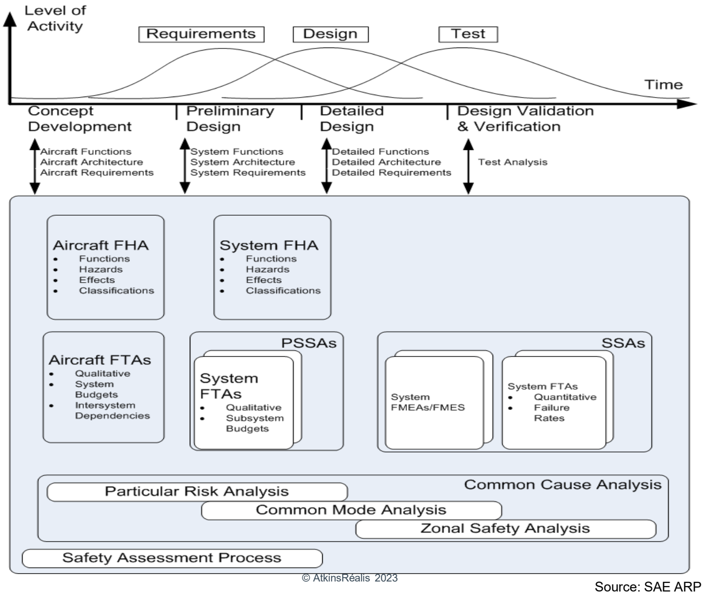
FHA Description – Hierarchy

- Start with a high level, qualitative assessment of the basic functions of the aircraft
  - Identifies and classifies failure conditions associated with aircraft level functions
- Fault Trees (FTs) are used to analyse the outputs from aircraft/system level FHA
  - Identifies which subsystem functions influence the aircraft level function being assessed
  - And so on to the component level
- Outputs from aircraft/system level FHA derive the starting point for safety requirement allocation
- Establishes aircraft safety requirements that must be satisfied e.g. from system level components .



AtkinsRéalis

Aircraft Safety Assessment Process



Source: SAE ARP 4761

AtkinsRéalis

FHA Process

Select system or subsystem:

- Identify all functions associated with the system
- Identify and describe all failure conditions associated with these functions
- Determine the effect of each failure condition based on the phase of operation
- Identify existing safeguards
- Identify additional credible safeguards

Record everything!

AtkinsRéalis

Example FHA Logsheet

Project: Aircraft Engine					Page No	
Description: The engine						
Ref	Function	Failure Condition	Phase	Effects	Safeguards	Recommendations
1.1	Push Aircraft	Loss of thrust				
1.2		Partial loss of thrust				
1.3		Thrust when not required				
2.1	Power Aircraft (Electrical)	Loss of electrical power generation				
2.2		Degraded electrical power generation				

AtkinsRéalis

Example FHA Logsheet

Project: Aircraft Engine					Page No	
Description: The engine						
Ref	Function	Failure Condition	Phase	Effects	Safeguards	Recommendations
1.1.1	Push Aircraft	Loss of thrust	Ground	No movement		
1.1.2			Taxi	Aircraft comes to halt safely		
1.1.3			Take-off	Aircraft unable to climb safely – collision into terrain		
1.1.4			Flight	Loss of thrust in-flight		
1.1.5			Landing	Unable to maintain speed above stall speed – collision into terrain		
1.2		Partial loss of thrust	Etc...			
1.3		Thrust when not required	Etc...			

AtkinsRéalis

Example FHA Logsheet

Project: Aircraft Engine					Page No	
Description: The engine						
Ref	**Function**	**Failure Condition**	**Phase**	**Effects**	**Safeguards**	**Recommendations**
1.1.1	Push Aircraft	Loss of thrust	Ground	No movement	-	-
1.1.2			Taxi	Aircraft comes to halt safely	-	-
1.1.3			Take-off	Aircraft unable to climb safely – collision into terrain	Multiple Engines	Improved reliability
1.1.4			Flight	Loss of thrust in-flight	Multiple Engines, Relight capability	Improved reliability Bail out capability
1.1.5			Landing	Unable to maintain speed above stall speed – collision into terrain	Multiple Engines	Improved reliability

AtkinsRéalis

FHA Workshop

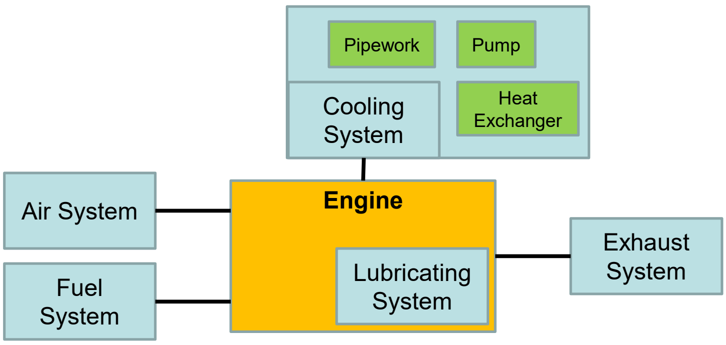
Plan Design Enable

FHA Workshop Lessons Learned

- Obvious failure mode is Fails OFF
  - Don’t naturally think of Functions failing ON (when not required)
- Phases of Flight adds granularity to the analysis
  - Naturally gravitate towards phase when function is required
  - FHA forces us to think of all scenarios (to identify all hazards)
- Can be used for on ground scenarios
- Allows us to design in safeguards and mitigations prior to introduction into service.

FMEA & FMECA

- Failure Modes and Effects Analysis is a **systematic**, bottom-up method of identifying the failure modes of a system to determine effects on higher parts of the system
- Failure Modes Effects and Criticality Analysis
  - An expansion on an FMEA whereby identified failure modes and causes of a system of equipment, are given severity and probability of occurrence.



Example FMECA – Engine

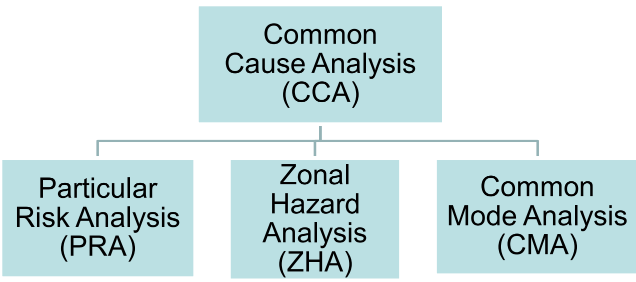
Equipment: Engine Cooling System Pump

ID	Function	Failure Modes and Causes	Mission Phase / Op Mode	Failure effects			Failure Detection	Compensating Provision	Severity Class	Probability	Remarks
				Local Effects	Next Higher Level	End Effect					
1	Operates to pump oil around engine	Impeller failure / Jam	Pumping	Impeller does not rotate	No oil flow through pump	No flow output from pump resulting in a loss of engine cooling	Pump BIT outputs fault.	Pump has operated on test for 2000hrs	CRIT	1.00E-07	
2		Continuous running due to hot short in motor	Pumping	Motor will not stop when commanded	Continuous oil flow through pump	Inability to isolate or stop flow when required	Dormant during operation. Pump BIT outpus fault on failure to stop when commanded	Pump has operated on test for 2000hrs	CRIT	3.68E-07	
3	Provide indications	Pump electronics fail to detect failure	Pumping	No detection of pump faults	Pump does not indicate fault status		PBIT, CBIT	Power up bit and continuous BIT should detect failures of the pumpt and provide an overall failure indication at pump level	CRIT	1.25E-08	
4		Pump electonics fail to ouput fault data								8.32E-06	
5		Sensor failure to detect incorrect state								1.00E-05	2 Redundant Sensors available

Risk Definitions: I – Intolerable; U – Undesirable; T – Tolerable; N - Negligible

Common Cause Analysis

- CCA includes three primary techniques to assess independence

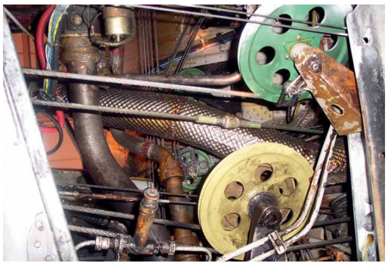


Particular Risk Analysis

- Assessment against a structured list of common types of risk to aircraft from outside of the system.
  - Examples are fire, leaking fluids, bird strike, tyre burst, high intensity radiated fields exposure, lightning, uncontained failure of high energy rotating machines, etc.

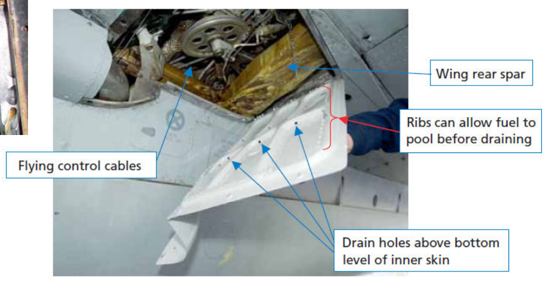
Zonal Hazard Analysis (ZHA)

- Other HAZID techniques do not typically address the interactions between systems and the environment
- ZHA is a **zonal** examination of the system to determine effects to and from other systems



The aim from the process is to reduce the potential for hazards from the co-location of equipment

Best used during the design phase

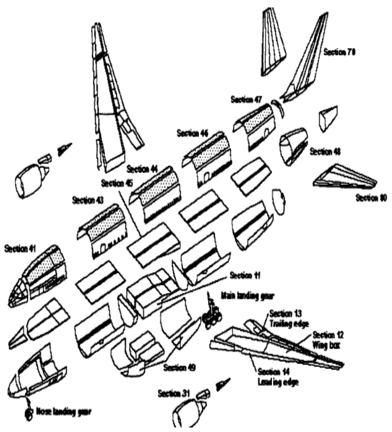


ZHA Process 1: Conformity to Design

- The first task is independent of the zones;
- Preparation of design and installation rules for each new system and the components within the system.
  - Details obtained from design drawings and installation instructions
  - Considerations from preliminary work
  - Aircraft level requirements and objectives
- Inspect the design against these rules for conformity

ZHA Process 2: Identification of Zones

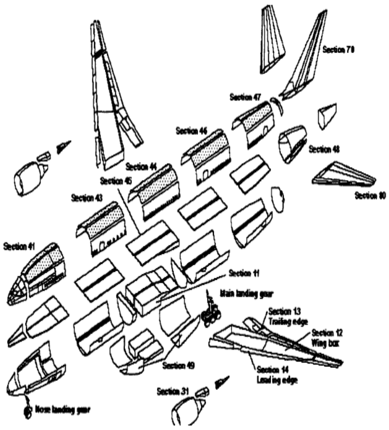
- Identify zones that reflect containment methods
  - Traditional compartmentalization of platform e.g. bulkheads, skin, etc
- Zones may be decomposed in a parent-child hierarchical order such as Major Zone, sub-major zone and then zone
  - To whatever level is meaningful
- Zones include all components of the platform including the skin of the aircraft.



AtkinsRéalis

ZHA Process 3: Determine Hazards

- Determine threats to system within selected zone
  - Fire, electrical short, power loss etc
- Determine effects on system / other systems in zone
- Determine effects on aircraft
- Determine mitigations
  - Eg containment mechanisms: Fireproof engine bulkheads, self sealing fuel tanks



AtkinsRéalis

Example ZHA Logsheet

Aircraft: Tornado			System: Engine bleed air Zone: Fuselage under Tail Fin		Issue: Date:
Ref	Failure component mode	Effect on System	Effect on Aircraft	Symptoms to 1. Flight crew 2. Ground crew	1. Crew Corrective Action 2. Aircraft condition after action
1					
2					

AtkinsRéalis

ZHA Example

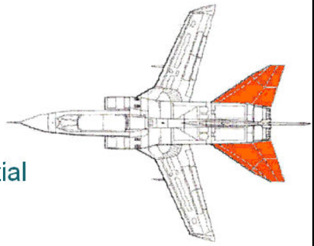
Aircraft ZHA Example

- Hot bleed air from engine used to feed ECS system in Tornado
- System provides high temperature & high pressure air via ducting that runs under the Fin assembly. This zone houses:
  - Primary Flying Controls and;
  - Electrical wiring looms.

AtkinsRéalis

ZHA Example

- Individual engine bleed air pipes connect at a T piece before routing bleed air forward. T piece also includes connection to Ground Pressurisation inlet. Joint between components sealed by asbestos gasket
- Failure of asbestos gasket could result in leak of high temperature & pressure bleed air into zone located under the Fin assembly
- Thermal effects could lead to failure of primary flying controls, electrical wiring loom, with potential to ignite Fin fuel tank.



AtkinsRéalis

Example ZHA Logsheet

Aircraft: Tornado			System: Engine bleed air Zone: Fuselage under Tail Fin		Issue: Date:
Ref	**Failure component mode**	**Effect on System**	**Effect on Aircraft**	**Symptoms to** **1. Flight crew** **2. Ground crew**	**1. Crew Corrective Action** **2. Aircraft condition after action**
1.1	Failure of bleed air T-piece gasket	Loss of hot bleed air from ECS pipe			
1.2		Thermal effects from escape of high temp/pressure air affects flying controls			
1.3		Thermal effects from escape of high temp/pressure air ignites fuel tank			
1.4		Thermal effects from escape of high temp/pressure air damages wiring loom			

SMT | Hazard Identification

AtkinsRéalis

Example ZHA Logsheet

Aircraft: Tornado			System: Engine bleed air Zone: Fuselage under Tail Fin		Issue: Date:
Ref	**Failure component mode**	**Effect on System**	**Effect on Aircraft**	**Symptoms to** **1. Flight crew** **2. Ground crew**	**1. Crew Corrective Action** **2. Aircraft condition after action**
1.1	Failure of bleed air T-piece gasket	Loss of hot bleed air from ECS pipe	Loss of ECS heating	Loss of cockpit heating	Assess impact on safety and mission
1.2		Thermal effects from escape of high temp/pressure air affects flying controls	Loss of control of aircraft	Loss of elevator control	Land as soon as practicable Consider ejection if aircraft uncontrollable
1.3		Thermal effects from escape of high temp/pressure air ignites fuel tank	Aircraft fire	Fire detection & warnings	Initiate fire suppression Assess impact on safety and mission
1.4		Thermal effects from escape of high temp/pressure air damages wiring loom	....	....	....

AtkinsRéalis

ZHA Workshop

Plan Design Enable

AtkinsRéalis

ZHA Workshop Lessons Learned

- Start small and grow outwards
  - Propagate the failure consequences outwards
- Go through the zone components systematically one by one
  - Make a list and tick them off
  - Use the checklist
- Prompts recovery actions instead of focussing on preventative controls
- Can be adapted to also target prevention controls.

PRA/ZHA Concluding Remarks

- Conformance to 'good' design practice is typical demonstrated by aircraft DO (confirmed by ITE)
- Zonal inspections should be carried out on the in-situ system once fitted to aircraft
- Further guidance to be found in ARP4761.

HAZID Techniques Overview

Technique	Scope	Advantages	Disadvantages
SWIFT	Equipment Hazards Holistic, high level	Easy, Intuitive, considers whole system	Does not tackle root causes, hazards can be missed
HAZOP	Equipment Hazards Component level, Bottom-up,	Can influence design, can apply to procedures	Takes time, can get lost in detail
FHA	Functional Hazards High Level system functions	Can influence design	Does not identify inherent equipment hazards
FMECA	Equipment Hazards Functional Hazards Component level, Bottom-up	Can influence design, Define maintenance policies	Relies on failure rate data, takes time, can get lost in detail, may not consider human factors
ZHA	Equipment Hazards External Influences	Considers system in-situ, good at identifying interactions with other systems, considers maintenance requirements	Requires expert input to recognise all hazards, little opportunity to influence design, requires access to aircraft
PRA	External influences	Considers external influences, Focuses on particular known hazards	Does not consider inherent equipment or functional hazards, might require detailed analysis

AtkinsRéalis

Have we Achieved the Learning Objectives?

- What is a Hazard?
- Why identify Hazards?
- What is the difference between SWIFT and HAZOP?

AtkinsRéalis

Questions

Plan Design Enable