B1

GUIDANCE MATERIAL:

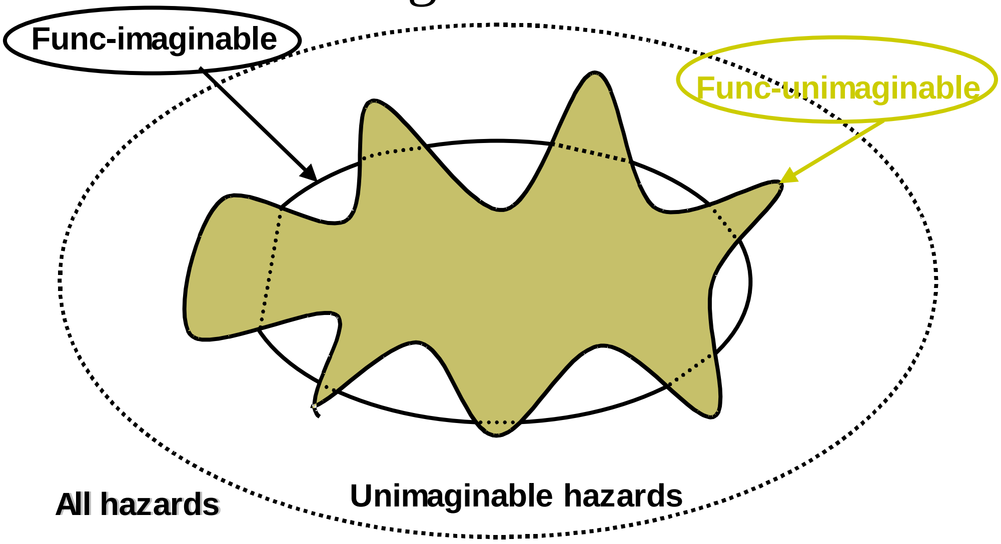
IDENTIFICATION OF FAILURE MODES, EXTERNAL EVENTS AND HAZARDS

1 IDENTIFICATION OF HAZARDS

Hazards can be identified by:

- systematically applying a list of key words, expressing the various failure modes, to each function of the system (See §2 of Guidance Material B1) ;
- systematically applying a list of external events to each function of the system (See §3 of Guidance Material B1);
- Using some abnormal occurrence/event scenario during brainstorming session to identify any additional "functionally unimaginable" hazards (See Guidance Material B2).

Functionally-imaginable & Functionally-unimaginable & unimaginable hazards



Guidance to plan hazard identification activities is described in Guidance Material A of SAM-FHA Chapter 2 and in Guidance Material B2 of this Chapter.

Hazards should be uniquely identified (ex: H-ACL-X) and should be traceable to abnormal events (when relevant).

Hazards should be labelled as described hereunder:

- [failure mode] of [(sub)-function] for more than [exposure time] in [Operational Environment]; or

- a “short story” including the hazard source (failure mode, external event, abnormal event scenario, combination of failure modes and/or events, …), the hazard mechanism (how it affects Air Navigation Service Provision including aircraft operations).

2 IDENTIFICATION OF FAILURE MODES

Some general categories of failure modes are listed in Table B1-1.

“Failure mode” is a prompt word to be used to identify hazards such as:

Total loss	Failure to start
Partial loss	Failure to stop
Error of input/ output:	Failure to switch
- missing data (partial loss, total loss)	Delayed operation (too late)
- detected erroneous/corrupted data (not credible error/corruption)	Premature operation (too early)
- undetected erroneous/corrupted data (credible error/corruption)	Inadvertent operation
- spontaneous data	Intermittent or erratic operation
- out of sequence	Modified operation
- out of range	Violation of operation (Routine or unintentional)
Misdirection of data	Misheard
Inconsistent information	Misunderstood
Erroneous updating	Used beyond intent
	Out of time synchronisation

Table B1-1. Examples of Failure Modes

Note: these failure modes are not specific to an architectural element only (technical or at ATCO or procedure level). For example corruption could be caused by lapses, slips of ATCOs or software corruption, mis-direction can be due to ATCO selecting the wrong call-sign or software corruption. However at FHA level, as the architecture is not yet known, this level of detail (cause of the hazard) is not addressed at this stage.

Virtually every type of failure mode can be classified into one or more of these categories, but the list is not necessarily exhaustive. The user should consider whether additional modes apply to the system being considered.

In addition, these generic definitions will sometimes be too broad for definitive analysis. Consequently, they will need to be refined and instantiated for the specific domain of application (e.g., communication, surveillance, etc.)

It will be also necessary to distinguish "detected" and "undetected" failure modes.

The list of failure modes covers both active and latent failures.

Active failures results from operational errors.

Latent failures results from errors or omissions during development (specification, design, implementation, integration and transfer to operations) and maintenance phase of the system life cycle.

For example,

- MISUNDERSTOOD has both an ‘active’ interpretation (e.g., ‘how might a controller misunderstand this alert?’) and a latent one (‘how might future users misinterpret the purpose of this procedure?’).
- USED BEYOND INTENT should prompt ideas about how a future operator might try to use (or misuse) the system in a way not considered by the designers.
- MODIFIED should prompt consideration of how future users might try to modify the system, without appreciating the design rationale.

Latent failures require particular attention and emphasis in FHA sessions, as it is generally much easier to think of active failures.

How to use?

Ideally, a detailed list of failure mode prompts, such as that in Table B-1 should be selected (meaningful to the system under assessment) and systematically applied to each function.

But it is recognised that this may not be practical, given the number of functions to be considered and the time available.

Where reduced lists of prompts are derived, it is helpful to draw the attention of FHA session participants to the full list, at least in the introduction to the session and possibly by providing handouts or other reminders for use during the session (see Guidance A).

3 IDENTIFICATION OF EXTERNAL EVENTS

A list of external events should be systematically applied to system functions in order to identify all hazards, since some of them may result from the interactions between the system and the environment of operation.

Examples of such external events, which should be taken into consideration in the process of identifying the hazards, are listed in the FHA - Chapter 1, Guidance Material A figure A-2.

4. HAZARD VERSUS SCOPE OF THE SYSTEM UNDER ASSESSMENT

When identifying hazards, different levels of hazards could be considered as a hazard is at the boundary of the scope of the system under assessment. Ideally hazards should be at the level of the Air Navigation System or Service. However if the scope of the system under assessment is reduced to a sub-level of this Air Navigation System or Service, the hazards will be identified at the boundary of that sub-system.

The Figure bellow illustrates that if the scope of the system under assessment is At level A (sub-sub-system), then what is considered as a hazard :

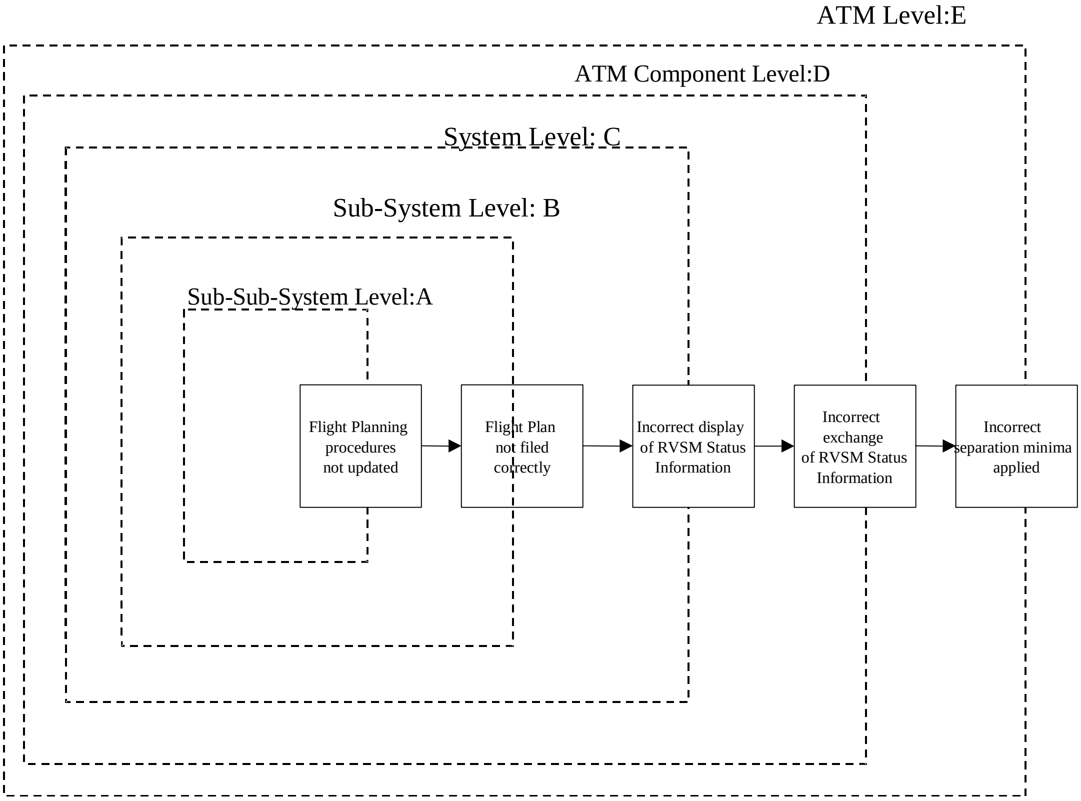

ATM Level:E
ATM Component Level:D
System Level: C
Sub-System Level: B
Sub-Sub-System Level:A
Flight Planning procedures not updated
Flight Plan not filed correctly
Incorrect display of RVSM Status Information
Incorrect exchange of RVSM Status Information
Incorrect separation minima applied

Figure B-1: Hazard at the boundary of the system under assessment

If the system under assessment is at lower level, such as sub-sub-system level A, for example if training programme for pilots should be changed due to introduction of RVSM, a hazard that could appear at the boundary of system “A” is “Flight Planning procedures not updated”.

But if the system under assessment is the FDPS (level C), one of the hazards identified could be “incorrect display of RVSM Status information”.

At the ATM Component level “D”, if the inter-centre co-ordination process is assessed, a hazard appearing at the boundary of that system “D” could be “Incorrect exchange of RVSM Status information”, which could eventually lead to the hazard at the highest level, ATM level “E”, that is “incorrect separation minima applied”.

The effect of this hazard at ATM level “E” (“incorrect separation minima applied”) could be an accident or incident.