Flight Operational Safety Assessment (FOSA) – a tool in establishing RNP AR Approaches

EASA Workshop, 20th October 2010

Edward Smith (DNV)
Presentation Contents

- What do the PBN manual and AMC 20-26 say?
- When and why is a FOSA needed?
- How should a FOSA be conducted?
- EUROCONTROL guidance document
- Lessons learnt so far
- Concluding remarks
PBN Manual and AMC 20-26

- **PBN Manual**
  - A FOSA should be conducted for RNP AR APCH procedures where aircraft specific characteristics, operational environment, obstacle environment, etc., warrant an additional review to ensure operational safety objectives are still achieved. The assessment should give proper attention to the interdependence of the elements of design, aircraft capability, crew procedures and operating environment.

- **AMC 20-26**
  - A FOSA should be conducted for each RNP AR approach procedure where:
    - More stringent aspects of the nominal procedure design criteria are applied (e.g. RF legs, RNP final approaches less than 0.3 and missed approaches less than 1.0)
    - The application of the default procedure design criteria is in an operating environment with special challenges or demands

- They do not say that a FOSA is needed for every RNP AR APCH procedure
Why is a FOSA needed?

- Procedure design – no buffers or tapering of obstacle clearance areas
- Curved paths (RF legs)
- RNP values on final approach below 0.15NM
- What happens, for example, if:
  - Undetected erroneous aircraft position calculation in one FMS - will aircraft remain within 2RNP?
  - Double FMS loss - will pilots be able to extract aircraft safely at all points on the approach?
  - High winds and precipitous terrain, etc.

With these challenging procedures, timely pilot inputs are even more critical.
Guidance on FOSA – How to conduct one?

- When the PBN manual and AMC 20-26 were being drafted there was not much guidance on FOSA
- 2-3 pages of helpful hints
- A number of stakeholders were asking “what do we need to do?”
- ICAO’s Instrument Flight Procedures Panel (IFPP) expressed concern about lack of guidance
- EUROCONTROL took action to address this concern in the absence of any other willing organisation at the time
Overall Approval Package

- FOSA is part of the overall documentation package, including:
  - Aircraft qualification and capability;
  - Procedure and airspace design;
  - Navigation data base validation programme;
  - Maintenance procedures;
  - Training (flight crew, dispatch, ATC);
  - MEL revision (as required);
  - Operational procedures requirements;
  - Conditions or limitations for approval;
  - Air traffic environment and operations; and
  - RNP monitoring programme.
Objectives of a FOSA

- The FOSA should ensure that for each specific set of operating conditions, aircraft and environment, all failure conditions are assessed and, where necessary, mitigations are implemented to meet the safety criteria.

- The assessment should give proper attention to the inter-dependence of the elements of procedure design, aircraft capability, crew procedures and operating environment.

FOSA acts as the glue, ensuring all these elements add up to a safe whole.
Examples of Dependencies - 1

- If there are aircraft failures or extreme operating conditions – do the flight crew know how to respond?

Diagram:
- FOSA
- Aircraft Performance
- Navigation/Information Services
- Infrastructure
- ATC Operations
- Operating Conditions
- Aircraft Failures
- Flight Crew Operations
Examples of Dependencies - 2

- If there are aircraft failures or extreme operating conditions – do the flight crew know how to respond?

- If ATC provides a clearance for an RNP AR APCH to an aircraft/crew not suitably equipped/approved do the flight crew know what to do?
Examples of Dependencies - 3

- If there are aircraft failures or extreme operating conditions – do the flight crew know how to respond?

- If ATC provides a clearance for an RNP AR APCH to an aircraft/crew not suitably equipped/approved do the flight crew know what to do?

- If there is an infrastructure problem, what information needs to be provided, does ATC know how to react, do flight crew know what the impact will be?

Such dependencies in context of a specific, potentially challenging, procedure where timely decisions could be critical.
EUROCONTROL Project Case Study 1 - Bastia

- Bastia, Corsica, France
- Working group members - DGAC/DSNA/Air France/Airbus/Thales
- Several iterations on the procedure design – all flown in simulator, Airbus A320
- Series of safety workshops – informal optimisation of design + formal FOSA sessions
EUROCONTROL Project Case Study 2 - Tromsø

- Tromsø, Norway
- Working group members - Luftfartstilsynet/ Avinor/ SAS
- Design submitted to ANSP and carrier at end of November 2008
- Simulator trials carried out in Jan 2009, Boeing 737NG
- Safety workshop in May 2009
- Test flights completed in Aug 2009
Key FOSA Characteristics

- Primarily an aircraft centred qualitative assessment
- However, needs to take account of factors outside the aircraft, e.g. ATC, procedure design, specific navigation infrastructure, etc.
- Historic reliance on subject mater expert assessment
- Relies on aircraft airworthiness certification process
- FOSA extends examination of hazards and mitigations
FOSA Steps - Overview

1. System definition
2. Setting safety criteria
3. Identification of hazards
5. Causal analysis & likelihood estimation
4. Consequence analysis
6. Determination of potential mitigations
7. Risk acceptability
8. Documentation of FOSA

Risk reduction measures

Meets criteria

Fails to meet criteria
FOSA Step 1

- **Step 1 System Definition**
  - Information to be gathered:
    - Procedure design
    - Aircraft, e.g. compliance against AMC 20-26
    - Flight crew & dispatch procedures and training
    - Proposed MEL
    - Nav infrastructure
    - ATC facilities
    - Airport and airspace environment
    - Etc.
  - Assumptions checklists (e.g. against AMC 20-26, section 4)
FOSA Step 2

- **Step 2 Setting Safety Criteria**
  - Primarily qualitative, e.g.
    - Risk Reduced As Far/ Low As Reasonably Practicable
    - Risk no greater than current operations
  
  - Quantitative, for equipment, e.g.
    - “The lateral excursions observed as a result of Probable failures should be documented against an objective of containment within 1xRNP”

1. System definition
2. Setting safety criteria
3. Identification of hazards
4. Consequence analysis
5. Causal analysis & likelihood estimation
6. Determination of potential mitigations
7. Risk acceptability
8. Documentation of FOSA

- Meets criteria
- Fails to meet criteria
- Risk reduction measures
FOSA Step 3

<table>
<thead>
<tr>
<th>Hazard Grouping</th>
<th>Hazard Ref.</th>
<th>Hazard</th>
<th>Reference / Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATC Operations</td>
<td>ATC 01</td>
<td>Procedure assigned to incapable aircraft</td>
<td>PBN / AMC 20-26</td>
</tr>
<tr>
<td></td>
<td>ATC 02</td>
<td>Inappropriate vectoring or “Direct To”</td>
<td>PBN / AMC 20-26</td>
</tr>
<tr>
<td></td>
<td>ATC 03</td>
<td>Separation or sequencing errors</td>
<td>Previous Eurocontrol Safety Case</td>
</tr>
<tr>
<td></td>
<td>ATC 04</td>
<td>Provision of incorrect pressure and/or temperature data</td>
<td>Previous Eurocontrol Safety Case</td>
</tr>
<tr>
<td></td>
<td>ATC 05</td>
<td>Lost communications</td>
<td>Previous Eurocontrol Safety Cases</td>
</tr>
<tr>
<td>Flight Crew Operations</td>
<td>FC 01</td>
<td>Erroneous barometric altimeter settings</td>
<td>PBN / AMC 20-26</td>
</tr>
</tbody>
</table>

- Step 3 Hazard ID
  - Group based workshops are an effective method
  - Mix of skills and knowledge
  - Supported by checklists

Example Hazard Checklist
FOSA Step 4

- Step 4 Consequence analysis

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Navigation database errors (NS 01)</th>
</tr>
</thead>
</table>
| Consequences                    | - Vertical or lateral deviation from intended route  
|                                 | - Loss of obstacle / terrain clearance |
| Consequential Mitigations       | - Reasonableness check of track angles and distances. Runway threshold co-ordinate check anchors this.  
|                                 | - VOR Radial check  
|                                 | - EGPWS / TAWS Class A |

Example Table
FOSA Step 5

- Step 5 Causal analysis

<table>
<thead>
<tr>
<th>Hazard:</th>
<th>Navigation database errors (NS 01)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Causes</td>
<td>Causal Mitigations</td>
</tr>
<tr>
<td>Procedure design error</td>
<td>• Followed ICAO PANS-OPS and PBN RNP AR Procedure Design Manual</td>
</tr>
<tr>
<td></td>
<td>• Verification of procedure design by peer review</td>
</tr>
<tr>
<td></td>
<td>• Flight test of procedure has been completed</td>
</tr>
<tr>
<td>Database out of date</td>
<td>• Airline AIRAC cycle update procedures</td>
</tr>
<tr>
<td></td>
<td>• Currency of database checked for entire flight (PBN 6.3.4)</td>
</tr>
</tbody>
</table>

Example Table

1. System definition
2. Setting safety criteria
3. Identification of hazards
4. Consequence analysis
5. Causal analysis & likelihood estimation
6. Determination of potential mitigations
7. Risk acceptability
8. Documentation of FOSA
**FOSA Steps 6 & 7**

<table>
<thead>
<tr>
<th>ATC Operations Hazards</th>
<th>Planned Causal Mitigations</th>
<th>Planned Consequential Mitigations</th>
<th>Potential Extra Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure assigned to incapable aircraft or crew (ATC 01)</td>
<td>- Flight Crew are responsible for declining inappropriate clearance</td>
<td>Go-around if approach is not fully prepared</td>
<td>In trial and early operations, flight crew will ask ATC for RNP AR approach. Will not be offered always on request.</td>
</tr>
<tr>
<td></td>
<td>- Flight crew check of AR equipment availability prior to approach</td>
<td></td>
<td>Special phraseology to be developed.</td>
</tr>
<tr>
<td></td>
<td>- Approach specific training for ATC (PBN 6.2.6)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Example Table

- **Step 6 Mitigations**
  - Document planned mitigations
  - Identify potential extra mitigations

- **Step 7 Risk Acceptability**
  - Look at hazard v mitigations balance
  - Determine mitigations which are required
FOSA Step 7 (cont’d)

Example Aircraft Failure Hazard

<table>
<thead>
<tr>
<th>Failures</th>
<th>Likelihood</th>
<th>Consequences</th>
<th>Extra Mitigations</th>
<th>Risk Acceptability?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undetected erroneous A/C position calculation in one FMS</td>
<td>SSA evaluated probability as Remote (between 10-5 and 10-7 per approach)</td>
<td>Contained within 0.4NM.</td>
<td>TAWS Class A</td>
<td>Specific procedure significantly less onerous than one used in airworthiness approval for AMC 20-26. Risk acceptable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implies RNP_{\text{non norm}} = 0.2NM</td>
<td>Contingency procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Demonstrated and documented in accordance with AMC 20-26</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
FOSA Step 8

- **Step 8 Documentation of FOSA**
  - Introduction (including justification for introduction of an RNP AR APCH, benefits etc.);
  - Description of the system (as per Step 1 above);
  - Overview of safety assessment process and safety criteria used;
  - Identification of relevant hazards, causes and consequences;
  - Documentation of relevant mitigations and determination of risk acceptability for RNP AR operations;
  - Key issues to be monitored;
  - Assumptions and open items to be validated and closed out;
  - Conclusions/ Recommendations;
  - Appendices with supporting information.
Linkage to AMC 20-26

RNP System Performance Analysis

Normal Aircraft Performance

Aircraft Failures Analysis

RNP\text{norm} \quad RNP\text{non norm} \quad \text{Ops Package}

AMC 20-26 Reqs.

- Analysis in context of demanding environment/procedure
- Failures based on existing SSAs

Flightdeck procedures and recommended training

OEM Certification

Aircraft Operator Approval

FOSA

- ATC Operations
- Nav Services
- Infrastructure
- Operating Conditions

In context of specific environment & procedure
Scale of FOSA

1. Potential for less detailed FOSA
   - Proposed RNP value for procedure
   - Operational Needs Analysis

2. Detailed FOSA

3. Not Achievable

Airworthiness Certification

RNP \text{non norm}

\begin{itemize}
\item e.g. 0.20
\item e.g. 0.10
\end{itemize}
Typical Participants in a FOSA

- FOSAs are often initiated by an Aircraft Operator (AO) wishing to obtain approval to fly an RNP AR procedure.

- In conducting the FOSA the AO will obtain inputs from:
  - Aircraft and Avionics Manufacturers; and
  - Air Navigation Service Provider (Procedure Designer, Air Traffic Controllers, Airspace Planners, Navaid Infrastructure Specialists, AIM Department, etc.).

- In addition various parts of an AO’s organisation will need to be involved, i.e. Flight Crew, Flight Operations Department, Dispatchers, Technical Support and Maintenance.
FOSA and the ANSP Safety Case

- When the RNP AR procedure is a new implementation this will represent an ATM change and an Air Navigation Service Provider (ANSP) may also be expected to undertake a safety risk assessment. For example a European ANSP will be expected to undertake a safety risk assessment compliant with ESARR4 or Commission Regulation No. 2096/2005.

- ANSP safety case for the RNP AR operation will draw on FOSA findings and will have to validate any ANSP-specific assumptions made during the FOSA (ATC phraseology, ATC contingency procedures etc)

- The ANSP safety case and the FOSA must be compatible
Approval Process – Seeking Efficiencies

- An approval is specific to a given combination of RNP AR approach, aircraft type and AO.

- This presents organisational challenges in the case of a foreign AO wanting to conduct an RNP AR APCH.

- It would be expected that the foreign AO liaise with the relevant European ANSP to ensure that their respective safety studies are consistent and to ensure that they will be allowed to use the RNP AR approach.

- This liaison may involve the ANSP or relevant regulator supplying information about what is required in the FOSA and what special safety requirements have been applied to other AOs using that particular RNP AR procedure.

- It would clearly be helpful if the FOSA conducted by the first AO to fly the RNP AR procedure was available to subsequent AOs, although it must be ensured that each AO complete the RNP AR implementation process fully.
Lessons Learnt

- Needs to be clear operational need for RNP AR APCH
- Value of early iterations
- Benefits of simulations
- Advantages of multi-disciplinary teams
- Impact of location specific factors
- Charting issues
Value of Early Iterations
Conclusions

- FOSA is a valuable tool in establishing the safety of RNP AR APCH operations and in facilitating approval.

- FOSA provides a systematic process for checking that risks are adequately mitigated across the range of hazards.

- EUROCONTROL’s FOSA guidance fills a gap and provides a tested basis for further development.

- Future guidance planned looking at RNP AR traffic separation applications and departures.
Safeguarding life, property and the environment

www.dnv.com