Minutes, ESARR6 – Review Meeting 22/1/2007

Minutes – meeting 22nd January 2007-01-22, Eurocontrol HQ

Florin Cioran, Chris Johnson and Tony Licu

Started 10.30

The main purpose of the meeting was to review the first draft of the guidance material submitted on the 22nd December, 2006. During the meeting we produced an annotated version of the first draft which is mentioned in the following minutes. The main tasks involved identifying links between the ESARR6 FAQs and with the guidance material for ESARRs 3 and 4.

All of the actions relate to Chris Johnson, except where explicitly stated.

General comments:
Florin mentioned that there are some problems with the text that was used in the guidance and the final boxes of ESARR6 – he will provide some updates possibly this is due to the guidance being started before the text of ESARR6 was finally agreed.

In the original guidance, sometime I go on to explain the explanation. Page 11, for example, the bullet pointed section after 'Therefore' in the initial draft.

The main problem is with the interpretation of the guidance it's not how to implement ESARR6 but for the regulator to help them oversee what should be the scope and so on. The language and the approach should be closer to that used in EAM3/GUI1 for example.

Check in all of the document for references to "particular lines of code" etc and make sure the references are more general, covering software functionality, documentation etc.

Possibly produce a correspondence diagram. Bring in more of the FAQs for ESARR6 into the guidance. What are the links with ESARR3 and 4 – provide a correspondence between the FAQ and the Guidance. Try to be consistent with the Guidance for ESARR3 and ESARR4.

SECTION 1 of the Draft Document – SCOPE:

Section 1.2 Interpreting the Document (page 7 of the draft)
This material is taken from the UK material and they already have guidance on INTERPRETING THE DOCUMENT. CAP670 page 150 in the PDF – PART2 REQUIREMENTS, 3.1 and so on. Also Appendix D, part B section 3. Look in table of contents for some reason it is listed under abbreviations.

Remove the section 6 in the guidance document entitled ADDITIONAL GUIDANCE – some ESARRs have these sections eg ESARR4 has a section called Additional Material but ESARR6 does not – we might decide to add it again later but there is no big need just now. **Or move material from page 10 there temporarily.**

ESARR4 Scope – Section 1.2 and 1.3 ESARR4 Guidance 1 – for the scope. 'Cover the human, procedural and equipment and the software' then say that ESARR6 takes the software further.

2.4.2 Elements about the lifecycle – not explicitly in ESARR6 but is important for the risk mitigation activities.

The FAQ material on the scope is already there – on page 8 of the current draft.

Get rid of the STCA reference

Delete material on page 11 and 12 that is providing guidance for the guidance.

FC Action:
ESARR6 paragraph iv on page 12 of the first draft – add something that ESARRs are not prescriptive but are objective based regulations. Florin will ask if there is something else to add here from an existing document. **Look at section 7 of the FAQ, page 13.**

Section 3 of the Draft – RATIONALE (page 14)

FAQ on page 7, "Why do we need…"
Add into the section on Rationale page 14 of draft 1.

Add a diagram showing the relationship between ESARR 3, 4 and 6 – see the FAQ page 9. There is an initial diagram on page 22 of draft 1 but it's not very detailed. Add explanation on the diagram. Show how they flow together.

Page 16 of the first draft get rid of the comment about hardware.

Page 17, get rid of the Geneva example. Remove comments on financial constraints and the paragraph on complexity because it deals more with the implementation of ESARR6.

Section 4 of the Draft – SAFETY OBJECTIVE (page 18)
Again there is guidance on guidance – Tony says to leave it in and get feedback during consultation. So we keep this but make some of the edits marked on the draft to allow quantitative risk assessments that will be supported by some ANSPs as the existing text is controversial.

Section 5 of the Draft – OBLIGATORY PROVISIONS (page 20)
Diagram and text on page 22 goes under 1.1 page 20.

Section 5.1, make it consistent with the full newer version of ESARR6 – sentence added about cutover after Ueberlingen – there are paragraphs from ED109 that can be added here.

Page 21-22 edits marked on copy, get rid of Guam example.

Paragraph 1.3 – make a link with ESARR 1, Section 7 – Safety Oversight of Changes not all changes need to be resubmitted – just those that relate to fatalities. Link to guidance material for ESARR1 where it is explained.

Section 2.2, page 25 applies only to changes to software not all existing ATM software-otherwise it would be too expensive.

See specific annotations on the document, need to generalize beyond specific examples that are included.

Make link about designated authority at the end of page 27 back to page 22 section 1.3 on the safety case issues – see annotation in the proofs.

Paragraph 2.6 on COTS page 29 of the draft guidance – integrate page 6 of the FAQ on COTS.

Avoid explicit reference to SAF.ET material because it is only one of several approaches that ANSPs could use.

ESARR6 Section 3: Requirements Applying to the Software Assurance Level

Section 3.1 needs to be updated – add also the section from page 20 of the FAQ and page 21 on the mapping from ESARR4.

Section 3.2 has changes from the draft guidance to the ESARR6 itself.

Sections 4.2 and 5.3 relate to the FAQ sections on completeness and correctness on page 17 so need to make the links here.

Page 32 – requirement is about software not just about safety so introduce material on FAQ page 16 here – not just about safety.

Consider color coding for different levels of explanatory material.

*****The meeting adjourned at 12.55 for lunch and resumed at 13.15*****

ESARR6 Section 6: Requirements…Software Configuration

The section that is written needs to be altered for the regulatory perspective. We need to include ‘what to look for’ and not ‘how to do it’. Also, need a stronger link to ATM lifecycle. SW01 CAP670 Section 9 and 10 part B section 3, p.22 and 23 – what the designated authority might expect. It’s a little bit too prescriptive though. ‘Guidance of Credible Arguments…’

6.3 This definitely applies to documentation for the software but does it also apply to wider forms of documentation? Florin thinks we need to ask for wider clarification – will check with Tony – can also consult other standards as well. Page 36 of the draft.

Page 37 of the draft, 8.2 needs to be added.

Old 8.2 becomes 8.3 – add in FAQs page 3, first four bullet points to be added for 8.3 on minimum standards – national bodies can ask for more but ESARR6 is the base line.

See also sections on applicability in appendix of ESARR6 which really just copy sections from ESARR3.