CAA Responses to Consultation Comments

Proposal

You said – A key point is the definition of "Design Organisation" and implications of this.

- **We acknowledge the comment, and the reference has been amended**

You said – Note that whilst no changes were proposed to GM1 ATM/ANS.OR.065(b) Occurrence Reporting SYSTEMS & CONSTITUENTS (a), we note that Systems are normally designed with redundancy and technically operate with reduced safety margins during the restoration period, what does impacting the "safety of the provision of the services" actually mean? We do accept that GM1 ATM/ANS.OR.065(b) Occurrence Reporting SYSTEMS & CONSTITUENTS (b) to (d) provide some clarity.

- **Our response – An example of impacting the "safety of the provision of services" is an increase to separation minima due to a failure.**

Response 1

You said – Change:

- Occurrence and Investigation reports should contain input from both an air traffic controller (ATCO) and an ATSEP when Air Traffic Service equipment or an ATSEP was a contributory factor to the occurrence.

To:

- Occurrence and Investigation reports should contain input from both an air traffic controller (ATCO) and an ATSEP when Air Traffic Service equipment or an ATSEP was a contributory factor to the occurrence. Alternatively, two reports can be submitted - one from the ATCO and one from the ATSEP.

Rationale:

- At our Unit, the ATE support is outsourced and there is no constant onsite precence of an ATSEP. Support can be provided via telephone etc. which would not meet the requirements of either of the new proposed paragraphs. In the case of telephone support, the ability of both parties to submit a report would continue to meet the aim of this amendment.
- **We acknowledge your comment and have amended the wording to address this type of situation.**

- You said – Whilst this is proposed as GM and so guidance only, it reads as AMC. We are therefore concerned as to expectations from CAA Inspectors with regards to compliance.
- **We acknowledge your comment and have amended the wording to reflect GM.**

You said – The guidance implies that an ATSEP is not expected to raise a report if they are present but are expected to do so when they are not present (and may have no direct knowledge of the event) – which seems illogical. What are the implications for Units without a permanent engineering presence? ATSEPs should participate in engineering investigations, but should only have to raise additional Reports where it would add value.

- **NATS comments at initial meetings with CAA were that due to SMCC maintaining a constant watch that a report was only required by an ATCO, the CAA agreed with this stance as there was no material benefit in dual reporting in this circumstance. Additionally we have amended the wording to give greater clarity.**
- **Units without a permanent engineering presence should only submit a report by ATCO/FISO/ATSA, with an engineering input into the follow up investigation report when Air Traffic Service equipment or an ATSEP may have contributed to the occurrence. Additionally we have amended the wording to give greater clarity.**

You said – Essentially, whilst we see this as Guidance and not obligatory, we disagree that the occurrence report has to contain input from both ATC and Engineering. The Occurrence report is there to record the event and to trigger an investigation which should consider all aspects of the event both ATC and technical.

- **We acknowledge your comments and have amended the wording to address this type of situation.**

You said – A joint occurrence report from both ATC and ATSEP could lead to an assumption that it is complete prior to the investigation and lead to premature conclusions by the Regulator.

- **The situation described alludes to the organisation not following the requirements for an investigation report post MOR being submitted. In this instance the CA would raise a finding against the organisation.**

You said – We do not object to whoever wants to raise a report can do but disagree with this being formalised as a regulatory requirement.

- **This is guidance material, if it were AMC or the Regulation it would be a requirement.**

You said – If there are concerns with the quality and coverage of our investigation reports then we need to focus efforts there.

- **The consultation has not cast any doubt on the quality and coverage of NATS investigation reports.**

Response 2

You said – (c) needs further explanation/clarification.

- **We acknowledge your comment and have amended the wording.**

You said – UK legislation/regulation does not define the term "Design Organisation" with respect to ATM/ANS Systems/Constituents, and the AMC should not be introducing such definitions; suggest the text in parenthesis is deleted.

- **We acknowledge your comment and have amended the wording.**

You said – If some additional guidance is to be provided regarding who has design responsibility, each Constituent should have a UK SoC (or a legacy Declaration) stating the "manufacturer", which is the organisation responsible for the design of the Constituent. However, each ANSP is responsible for the design of their System.

- **We acknowledge your comment and have amended the wording.**

You said – Safety is the ANSP's responsibility and the relationship with manufacturers is contractual; there is no inherent legal obligation for a manufacturer to make changes to their products based on these reports, and presumably this AMC is not intended to introduce an obligation for an ANSP who experienced a reportable occurrence to pay for a manufacturer to make changes. Hence this has the potential to be more paperwork for no clear purpose.

- **This is not the intent of the proposed change. The intent is for accurate MTBF/Availability data to be available to ANSPs when procuring systems. If the manufacturer is unaware of outages the data supplied is inaccurate.**

You said – ANSPs may have contractual mechanisms in place to request changes to ensure we provide a safe service, but the manufacturer may not even exist or the ANSP may choose to use other mitigations or even procure an alternative product as a backup, etc. On this basis, NATS are not convinced there needs to be a generic obligation to report occurrences to manufacturers, as the manufacturers have no obligation to make any changes; there is an obligation on the ANSP to ensure they provide a safe service, and raising defects with the manufacturer may or may not be an appropriate part of this depending on the contractual relationship.

- **The intent is for accurate MTBF/Availability data to be available to ANSPs when procuring systems. If the manufacturer is unaware of outages the data supplied is inaccurate.**

You said – Regarding the obligation to report to "any other organisation that has a service reliant on those systems and constituents", it is not clear if this means reporting to other organisations which use the service provided by the ANSP, or reporting to other organisations that make use of

the same Constituent; if the latter, the ANSP is unlikely to have this information (the manufacturer may know, but I suspect there is no mechanism in the current legislative framework to require them to notify other users of their products).

- **We acknowledge your comment, and this element has been removed.**

Response 3

You said – This establishes the need for the ANSP to agree which failures are reportable with the competent authority, but neither the AMC or guidance material details the mechanism for doing this, noting it could become onerous and complicated, especially if this is to be formally documented for every Constituent, and it could result in ANSPs reporting different things. Rather than pushing this out to individual ANSP agreements (potentially at Constituent level), the AMC/GM should aim to more clearly define the types of failures which must be reported.

- **The UK has >60 ANSPs and each ANSPs operation is unique; for a CA to attempt to devise a single set of circumstances where occurrence reporting is required that fits all is not possible. The ANSP is in a better position to determine what is reportable in accordance with 376/2014, 2015/1018 and 2017/373 and submit for acceptance.**

You said – NERL has tried to agree a list of failures over the last 18 months and this has proven to be too complex. The first challenge is around the concept; NATS believes this reporting is about Safety and the potential safety impacts. Whereas the view we took from the CAA was it wider than that and covered resilience. We need to first agree the principles as an exhaustive set of systems/scenarios is unlikely to work.

We concur that the reporting is about safety and potential safety impacts, the intent of this regulation is not to include resilience, unless loss of resilience impacted safety or had a potential safety impact.

Response 4

You said – What evidence is required as to what is on the list?

- **On completion of the consultation, we will issue instructions as to how ANSPs should inform us of the circumstances that they will report.**

You said – Do we currently have a list?

- **We are unable to answer this question.**

You said – 2(ii):

Should "i.e." be an "e.g."?

- **Noted – changed to e.g.**

No definition for increase in controller workload – many of our incidents involve an increase in controller workload, but they are mainly within capacity and therefore not service affecting. For the example provided, this will mean a huge increase in investigator workload if the depth of investigation has not been pre-agreed beforehand to only report that an event has occurred. Perhaps this should be limited to, for example, occurrences where non-standard or major ATC fall-backs have been required to resolve the situation.

We acknowledge your comment and have amended the wording to provide an example of increased workload. As stated in the proposed amendment to GM1 ATM/ANS.OR.A.065(b) Occurrence reporting (b), it is for the Service Provider to propose what they deem is reportable, therefore the scenario you are describing may be avoided by the acceptance of your submission.

You said – 2(iii):

Is "Complete failure" is acceptable? E.g. partial failure could also meet the criteria defined here. This needs to be clarified.

Not sure what is meant by 'failure during a maintenance activity' – maybe a failure of a maintenance activity that was intended to be non-service affecting?

Regarding the outside operational hours example – we should not have to report issues that could have only occurred outside operational hours (e.g. due to maintenance planned to be out of hours in case something unintended occurred).

- **We acknowledge your comment and have amended the wording to complete or partial failure.**
- **For clarity, failure during maintenance, or outside of operational hours, which prevents the system being available for use that may have a safety impact, or a potential safety impact.**

You said – 3:

Is the expectation that such reports are submitted by the Service Provider or the 3rd Party?

How does this impact us for equipment failures within the CPDLC network? Do we have to report failures that we don't see in NATS but still meet the test in (iii)

- **This is not intended for CPDLC or similar supplied services. If an ANSP subcontracts a service to another organisation, the organisation that provides the service should report in accordance with the contracting ANSPs procedures.**

You said – As a general point, the requirement is for "ATM/ANS" i.e. applicable to all services including AIS, MET, etc. but (with the exception of ILS). The guidance seems to be focused on ATS; what types of failures need reporting for other services?

- **2017/373 states - A service provider shall report to the competent authority, and to any other organisation required by the Member State where the service provider provides its services, any accident, serious incident and occurrence as defined in Regulation (EU) No 996/2010 of the European Parliament and of the Council and Regulation (EU) No 376/2014.**

Response 5

You said – Is the implication that ANSPs need to update their IOP Technical Files to capture where the ANSPs have design responsibility, and in this case, does the ANSP need to write a new SoC?

There is a concern around how we specify the designer for systems that are based on COTS Hardware, supplier installed OS or software and NATS specific adaptation. Who holds the accountability for the overall design? We would argue NATS does.

- **We acknowledge your comments and this aspect has been removed due to it being covered elsewhere in UK regulations.**

Response 6

You said – As mentioned above, AMC/GM should not be defining new terms; calling the manufacturer a "DO" almost suggests that they have legal obligations/privileges beyond their contract with the ANSP, which is not the case. On this point, there is no legislative obligation for the manufacturers to perform any trend analysis or indeed take any action based on these reports. In general, any "reporting" to the manufacturer should go through the ANSP's Design Authority rather than an ATCO/ATSEP, and their report would contain very different information than a report to the CAA, e.g. detailed technical information, possibly log files, etc.

The reference to "external assistance" is possibly a different issue, i.e. ensuring appropriate 3rd line support; NATS does not think this Occurrence Reporting requirement is intended to cover maintenance arrangements, which is a separate issue that needs to be contractual agreed.

NATS does share the more significant fault data with suppliers, however there is an important caveat that need to be considered. Whist a piece of equipment maybe provided by a supplier, often NATS creates a layer of adaptation on top of the system and if the fault lies within that area unless we felt relevant to the underlying system we would not share.

- **We acknowledge your comment and have addressed the DO aspect in the preceding responses.**
- **We acknowledge your comment and have removed the external assistance element.**
- **We do not disagree with this concept, where NATS creates a layer of adaptation and the fault occurs within that layer, then it is the responsibility of NATS and therefore not a requirement to involve the supplier of the other parts of the system.**