Annex to ED Decision 2020/006/R

'AMC/GM to Part 21 — Issue 2, Amendment 10'

The text of the amendment is arranged to show deleted, new or amended text as shown below:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in blue;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

Annex I to ED Decision 2012/020/R of the Executive Director of the Agency of 30 October 2012 is amended as follows:

1. Appendix A to GM 21.A.91 is amended as follows:

Appendix A to GM 21.A.91 Examples of Major Changes per discipline

[…]

4. Systems

[…]

For other codes, the principles noted above may be used. However, due consideration should be given to specific certification specifications/interpretations.

In the context of a product information security risk assessment (PISRA), a change that may introduce the potential for unauthorised electronic access to product systems should be considered to be 'major' if there is a need to mitigate the risks for an identified unsafe condition. The following examples do not provide a complete list of conditions to classify a modification as major, but rather they present the general interactions between security domains. Examples of modifications that should be classified as 'major' are when any of the following changes occur:

— A new digital communication means, logical or physical, is established between a more closed, controlled information security domain, and a more open, less controlled security domain.

— For example, in the context of large aircraft, a communication means is established between the aircraft control domain (ACD) and the airline information services domain (AISD), or between the AISD and the passenger information and entertainment services domain (PIESD) (see ARINC 811).

As an exception, new simplex digital communication means (e.g. ARINC 429) from a controlled domain to a more open domain is not considered as major modification, if it has been verified that the simplex control cannot be reversed by any known intentional unauthorised electronic interaction (IUEI).

— A new service is introduced between a system of a more closed, controlled information security domain and a system of a more open, less controlled security domain, which allows the exploitation of a vulnerability of the service that has been introduced, creating a new attack path.

For example:

- opening and listening on a User Datagram Protocol (UDP) port in an end system of an already certified topology;
- activating a protocol in a point-to-point communication channel.

- The modification of a service between a system of a more closed, controlled security domain and a system of a more open, less controlled security domain.
- The modification of a security control between a system of a more closed, controlled information security domain and a system of a more open, less controlled security domain.

5. Propellers

[…]