



FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 3: Air Navigation System Performance Improvement

3.1: Proposals to improve the efficiency of air navigation services contributing to LTAG

AIM PRODUCTS IMPROVEMENT WITH DATA INTEGRITY ASSURANCE

(Presented by the United Arab Emirates)

EXECUTIVE SUMMARY

This paper presents the United Arab Emirates' initiative and experience in improving the provision of aeronautical information products and reducing reliance on traditional, often environmentally taxing, methods. It demonstrates a forward-thinking approach to embracing digital technologies.

1. INTRODUCTION

1.1 As per Annex 15 — *Aeronautical Information Services* states that the integrity of aeronautical data shall be maintained throughout the data chain from origination to distribution to the next intended user. Digital data error detection techniques shall be used during the transmission and/or storage of aeronautical data and digital data sets. While data integrity (assurance level) is defined as a degree of assurance that an aeronautical data and its value has not been lost or altered since the origination or authorized amendment.

1.2 As per *Procedures for Air Navigation Services — Aeronautical Information Management (PANS-AIM)* (Doc 10066) data integrity should be assured by employing cryptographic technologies (e.g. hash functions, message authentication codes, asymmetric and symmetric encryption, and digital certificates). The technical means used for data error detection should be based on the use of systematic cycling codes. The means to implement systematic cycling codes include the use of hash functions and cyclic redundancy check (CRC). While CRC is defined as a mathematical algorithm applied to the digital expression of data that provides a level of assurance against loss or alteration of data.

2. DISCUSSION

2.1 When complex mathematical algorithm cannot be applied due to lack of guidance, technology or expertise, assuring Data integrity of provided aeronautical information was decided to be the use of unalterable media (e.g. CDs or DVDs). However, this approach was identified as having its own

challenges which are human resource, time resource and financial resource. In addition and most importantly it impacts environmental sustainability goals due to the use of plastic, paper and ink.

2.2 The quickest and most efficient means is the distribution of aeronautical information using the internet. This comes with risk of errors and data corruption while downloading from websites

2.3 Hence the United Arab Emirates' aeronautical information management (AIM) researched and identified that message-digest 5 (MD5) cryptographic hash algorithm can be used to authenticate files. The MD5 hashing algorithm uses a complex mathematical formula to create a hash. It converts data into blocks of specific sizes and manipulates that data a number of times. While this is happening, the algorithm adds a unique value into the calculation and converts the result into a small signature or hash.

2.4 An in-house build windows application was developed to generate hash code for each individual files within the aeronautical information package. A list of each file's hash code along with instructions (commands) for decoding is provided in the package, which the customer can use for data integrity assurance. They users can check the integrity of all files or randomly any individual files using the list provided within the package.

2.5 Also a single hash code is generated for the zip file of the entire aeronautical information package which is provided on the website. The single hash code and instructions for decoding is provided in the email notification of the aeronautical information update. The recipients can use the instructions to assure data integrity of the downloaded package before even using it.

2.6 The commands for generating and checking the implemented hash codes run without the need for any additional software.

3. CONCLUSION

3.1 The meeting is invited to note the United Arab Emirates' experience and achievements such as eliminating outdated technology, environmental sustainability, improving customer experience and optimize resource.

3.2 The meeting is aslo invited to consider forward-thinking approaches to embracing digital technologies for further improvement.

— END —