Agenda Item 4: **Assessment of operational requirements to determine the implementation of improvements in communication, navigation and surveillance (CNS) capabilities for operations in route and terminal area**

FOLLOW UP TO PERFORMANCE AND ACTIVITIES OF REDDIG II

(Presented by the Secretariat)

SUMMARY

This working paper presents information on performance and activities carried out since the Nineteenth Workshop/Meeting of the SAM Implementation Group (SAM/IG/19).

References

- Contract REDDIG 22501200;
- Report of the Twentieth meeting of the REDDIG Coordination Committee (RCC/20) (Lima, Peru, 21-23 March 2017);
- Nineteenth workshop/meeting of the SAM Implementation Group (SAM/IG/19) (Lima, Peru, 22-26 May 2017); and
- Sixth meeting on the technical-operational implementation of REDDIG II (RTO/6) (Manaus, Brazil, 12 June 2017).

ICAO strategic objectives:	*A – Safety* *B – Air navigation capacity and efficiency*

1. Background

1.1 The SAM/IG/19 meeting analysed the performance and activities of REDDIG II since the SAM/IG/18 meeting, highlighting the increase in REDDIG II availability since August 2016, upon completing the implementation of changes to LNBs (low-noise block converter).

1.2 Likewise, the meeting took note of the initial REDDIG II security analysis conducted by the *ad hoc* group, made up by Argentina, Brazil, Colombia, French Guiana (France), Paraguay, and Peru, and of the need to draft an action plan specifying the dates for the implementation of the proposed actions to mitigate identified threats that might affect REDDIG II security.

2. Discussion

2.1 The main activities carried out in REDDIG II, as agreed at the last meeting of the Committee, are presented below, as well as an analysis of its performance since the SAM/IG/19 meeting. The description covers mainly the following aspects:

a) REDDIG II training programme;

b) REDDIG II operation and analysis of the implementation of new services.

REDDIG II training programme

2.1. Regarding training activities, the following courses were delivered:

c) Advanced course on REDDIG II operation
d) Course on IP networks, applied to the REDDIG
e) Course on network fundamentals (basic) for personnel of the Manaus NCC

Advanced course on REDDIG operation

2.2 This course was addressed to the technical staff responsible for the operation and maintenance of the REDDIG II station that had previously attended the basic courses. Among the aspects covered, the course emphasised the operation and management of the Skywan 1070/7000 modem, with a theoretical-practical description of the '*Line Up Manager'* software, as well as troubleshooting of station components.

2.3 This course was delivered on 13-16 June 2017 at the premises of the Training and Technical Updating Section (*Sección de Instrucción y Actualización Técnica* - SIAT) of the Fourth Integrated Centre for Air Defence and Air Traffic Control (*Cuarto Centro Integrado de Defensa Aérea y Control del Tránsito Aéreo* – CINDACTA IV), Manaus, Brazil. For this event, one fellowship was granted per member State of Project RLA/03/901, and simultaneous interpretation services were provided.

2.4 The course was attended by 36 delegates of Argentina, Brazil, Chile, Colombia, Ecuador, Guyana, Paraguay, Peru, Suriname, Trinidad & Tobago, and Venezuela. Participants received a digital version of the content, as well as supplementary electronic files.

Course on IP networks, applied to the REDDIG

2.5 The course was addressed to technical staff with IP network knowledge that had participated in the courses "*Interconnecting Cisco Network Devices Part 1 (ICND1)*" and "*Interconnecting Cisco Network Devices Part 2 (ICND2)"*, and was responsible for the operation and maintenance of the REDDIG II station.

2.6 The course was held on 13-17 November 2017 at the facilities of the Training and Technical Updating Section (*Sección de Instrucción y Actualización Técnica* - SIAT) of the Fourth Integrated Centre for Air Defence and Air Traffic Control (*Cuarto Centro Integrado de Defensa Aérea y Control del Tránsito Aéreo* – CINDACTA IV), Manaus, Brazil. For this event, one fellowship was granted per member State of Project RLA/03/901, and simultaneous interpretation services were provided.

2.7 The content was based on the lessons learned from the Cisco ICND1 and ICND2 courses, but focusing on the equipment and services being provided in REDDIG, with virtual laboratories using the "*Packet Tracer*".

2.8 The course was attended by 24 delegates of Argentina, Brazil, Chile, Guyana, Paraguay, Suriname, Trinidad & Tobago, and Venezuela.

Course on network fundamentals (basic) for the personnel of the Manaus NCC

2.9 This course was addressed to personnel working at the Manaus NCC, and was consistent with the commitment of the project to continuous training. This course was not in the plan of activities defined by the RCC/20, but was considered necessary. It entailed no cost for the project.

2.10 The purpose of the course was to refresh and supplement fundamental and advanced concepts on transmission systems for voice and data transmission applied to civil aviation.

2.13. The course scheme was based on network fundamentals oriented to the aeronautical applications over IP of Project RLA/03/901 of the ICAO SAM Office, on the CCNA (*Cisco Certified Networking Associate*) technical-practical course *Networking Fundamentals*, and on different sources that address telecommunication issues in a logical manner.

REDDIG II operation and analysis of the implementation of new services

REDDIG II Brasilia node

2.15 The Brasilia node became operational on April 2016. However, some problems were observed during its operations that needed to be corrected.

2.16 In this regard, a mission was conducted to Brasilia on 16-25 October 2017, with the participation of the REDDIG Administration, INEO and personnel of CINDACTA I.

2.17 In summary, tasks involved the following areas:

a) verification of the condition of serial cables and the operation of chain B
b) issues with maintenance and administrative voice circuits
c) verification of coaxial cabling
d) causes of packet losses in the Skywan A modem
e) verification of Gorgy Timing operation
f) server backup procedures in external disks
g) full, overall verification of the operation of the station and its components

2.18 Tasks performed during the mission resolved the last problems still pending in the REDDIG II node in Brasilia, leaving pending the definitive resolution of a problem with the 10Mhz connection. However, a temporary solution was found with the installation of a DC-Block in the Tx path of the 10MHz connection. One DC-Block was not enough.

2.19 This DC Block had to be replaced by four definitive DC-Blocks, adapted to the frequency range of the REDDIG system. To this end, INEO sent four DC Blocks BLK-6-N + (mini-circuits) to the location SBBR. These were definitively installed on 10 January 2018, which resolved all the problems in the Brasilia station.

REDDIG II nodes

2.20 During the mission to Brasilia, issues related to the network in general were addressed.

2.21 In this regard, in addition to the aforementioned tasks involving the Brasilia node, the following tasks were fulfilled:

a) Verification of the operation of the NMS of Venezuela and Ecuador
b) Analysis of operational instability in Venezuela
c) Support to NDSatCom
d) Verification of the operation of the La Paz node
e) Issues in the Ezeiza station
f) Establishment of a bandwidth utilisation calculation procedure

2.22 In the particular case of Ezeiza, it was an event that occurred during the mission, and was caused by weather conditions that affected the station during the night of 18 to 19 October 2017.

2.23 Regarding support to NDSatCom, this refers to action taken to facilitate remote access by the personnel of said company to the Skywan A modem of Manaus to solve the periodic freezing problem in the equipment.

Problems in the IBUC of Suriname and the modem of Bolivia

2.24 On 17 October 2017, IBUC B of the Paramaribo node (Suriname) failed. Although all the corresponding actions were taken to restore functionality, it was necessary to coordinate with INEO for delivery of the equipment to the factory for repair and dispatch of a spare 80W IBUC from the Regional Office in Lima. The equipment sent from the SAM Office remained in customs in Paramaribo for five months. It was finally released and installed on 7 May 2018.

2.25 The La Paz modem (Bolivia) failed on 15 June 2017. The Regional Office sent a modem to La Paz, which, after some logistical problems in Bolivia, was finally received in November and installed at the station on 20 November 2017. The failed equipment was dispatched from Bolivia, through INEO, to the factory for repair.

Final acceptance tests of REDDIG II (FNAT)

2.26 The provisional acceptance tests of REDDIG II (doc PSAT – NAT - 2022 NT - 2141167C Rev. H) were conducted on 31 January to 5 February 2015. Once tests were completed, the focal points of REDDIC II member States signed the PSAT certificate, with comments on each node.

2.27 The PSAT results with the comments on each node were recorded in the PSAT document (version H). This document was posted on: www1.lima.icao.int/reddig.

2.28 According to article 13.1 of contract Nº 2250120 (Provision of a new regional telecommunications network (REDDIG II)), the INEO&Level 3 consortium had 40 days to correct the deficiencies identified during the PSAT. Within the 40-day period, the INEO&Level 3 consortium corrected many of the deficiencies, except for the following major failures:

- Random freezing of the satellite modem (Skywan ID 1070) at some of the REDDIG II nodes
- Random freezing of the satellite modem of Manaus, chain A (Skywan ID 7000)

2.29 The INEO&Level 3 consortium finished correcting these major failures in late 2017. In this regard, the final acceptance tests of REDDIG II (FNAT) were conducted on 29-30 January 2018, and the FNAT certificate was signed on 30 January. This activity took place at CINDACTA IV facilities in Manaus, Brazil, where the REDDIG II node of Manaus and the NCC are located.

Implementation of new services

2.30 Since the RCC/20 meeting, the following AMHS circuits have been implemented and commissioned in REDDIG II:

Brasilia - Bogota (May 2017)
Brasilia - Georgetown (July 2017)
Bogotá - Caracas (December 2017)
Brasilia - Caracas (March 2018)
Brasilia –Ezeiza (March 2018)

2.31 Likewise, other AMHS circuits were implemented but are not yet in operation. They are expected to be operational over the course of 2018:

Ezeiza - Lima
Ezeiza - Santiago
Ezeiza - Montevideo
La Paz - Lima
Lima - Guayaquil
Bogotá - Guayaquil
Caracas - Guayaquil
Bogotá - Panama (MEVAIII REDDIG II interconnection)
Brasilia - Montevideo

2.32 Likewise, connections were established at the level of the network for the exchange of radar data between:

Ezeiza - Santiago
Ezeiza - Asunción

It is expected that the exchange of radar data between the aforementioned locations will become operational in 2018.

Availability of REDDIG II

2.33 **Appendix A** to this working paper contains a table showing the availability of REDDIG since the beginning of operations. The table shows that during the first two years of operation of REDDIG II (2015 and 2016), due to initial adjustment issues, availability levels were below 99.99%. However, after 2016, once random freezing problems in satellite modems were solved, availability reached the expected level of availability of more than 99.99%.

Analysis of REDDIG II security

2.34 The Sixth meeting on the technical-operational implementation of REDDIG II (RTO/6) presented an initial action plan for the adoption of measures to mitigate identified threats which might affect REDDIG II security, as shown in **Appendix B** to this working paper.

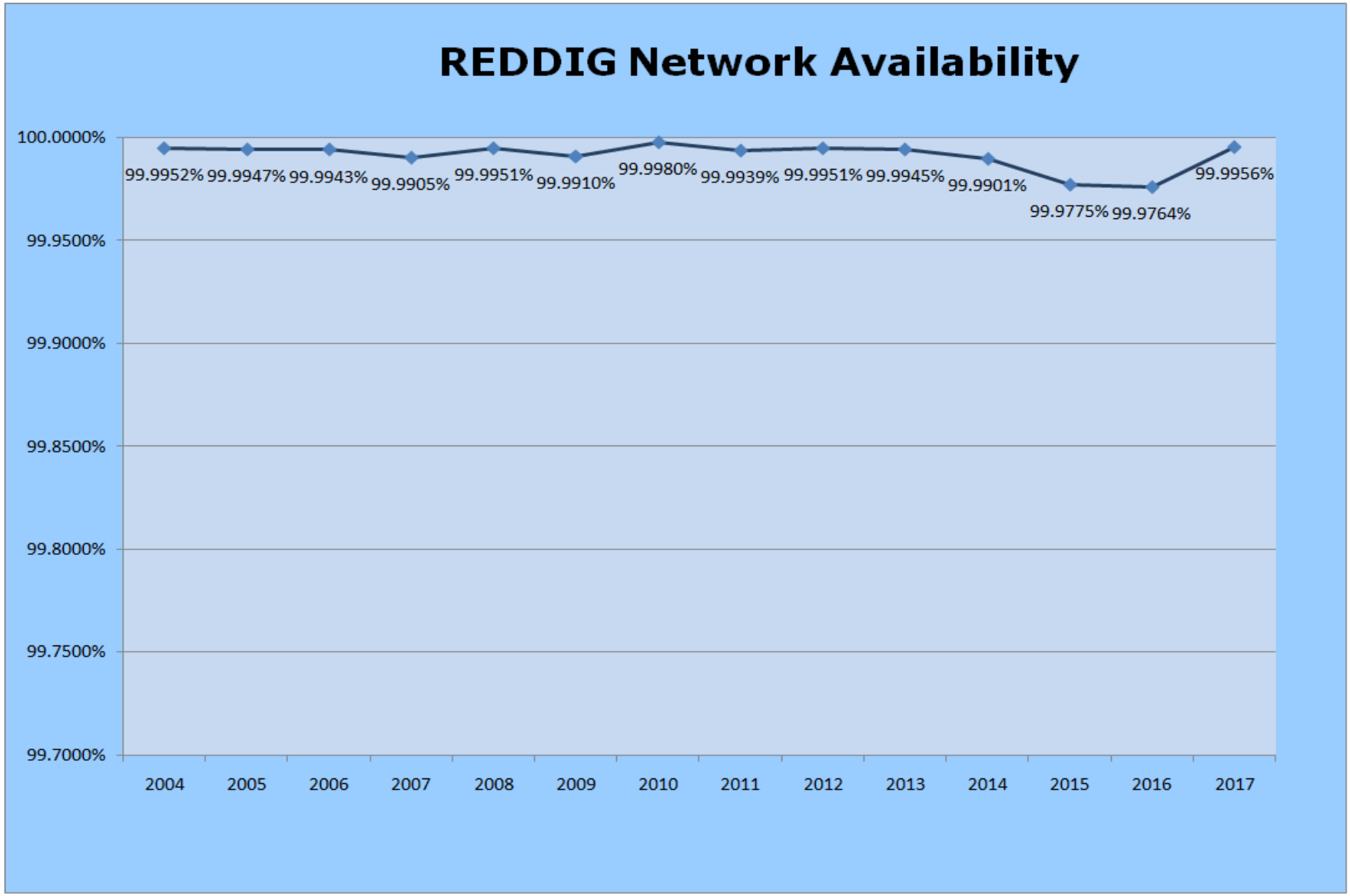
3 Suggested action

3.1 The Meeting is invited to:

a) take note of the information provided herein;

b) review the activities carried out and the performance of REDDIG II since the SAM/IG/19 meeting, as shown in section 2 and the corresponding **Appendices A and B** to this working paper; and

c) discuss any other matter it may deem appropriate.


REDDIG Network Availability
100.0000%
99.9500%
99.9000%
99.8500%
99.8000%
99.7500%
99.7000%
99.9952%
99.9947%
99.9943%
99.9905%
99.9951%
99.9910%
99.9980%
99.9939%
99.9951%
99.9945%
99.9901%
99.9775%
99.9764%
99.9956%
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

APPENDIX B

Security Analysis of REDDIG II

1 Introduction

1.1 Based on what was established in the teleconference of May 5, 2017, related to Conclusion RCC/20-3, Security Analysis of REDDIG II (formulated at the Twentieth Coordination Meeting of REDDIG - Project RLA/03/901 (RCC/20), and the work being done by the ad hoc group nominated at the Nineteenth REDDIG Coordination Meeting, with the objective of analyzing the security of REDDIG (conformed by Argentina, Brazil, Colombia, French Guiana (France), Paraguay, Peru and the Secretariat) to prepare a plan of action, specifying implementation dates for proposed actions, which are presented as Appendix H to the Agenda Item 3 of the final report of the RCC/20.

Action plan for the implementation of the security analysis of the REDDIG II

REDDIG II threats

1.2 Regarding the REDDIG II internal threats analysis, it was recalled that in each of the REDDIG II nodes should be installed redundant routers together with an "Ethernet switch", which will support all the "VLANs" of all IP services, the current and the future ones. This requirement was formulated at the third operational technical meeting of REDDIG through Conclusion RTO/3- *Installation of a router and redundant Ethernet switch for native IP services*

1.3 In order to standardize the configuration of the routers and switches, their technical characteristics, IP addressing, firewall, NAT application and other protocols, **an initial study** is presented below. This initial study will be distributed to delegates of the ad hoc group for their comments and **will be presented to the Sixth Operational Technical Meeting of REDDIG II** to be held in Manaus Brazil from June 12 to 16, 2017 for review. This study will subsequently be presented at the RCC/21 (March 2018) **for approval of the implementation** as an extension of the REDDIG II contract.

2. Initial Study

2.1 Timely it was established that all States should have implemented edge routers and it could be assumed that not all nodes have performed this action.

2.2 As mentioned in different circumstances, security in REDDIG II should be defined as the process by which resources are protected. Security objectives should be :

1) Protect confidentiality.
2) Maintain integrity.
3) Ensure availability.

2.3 Objectives that determine the imperative to protect the entire network in order to avoid threats and vulnerabilities.

2.4 A threat is an unauthorized access to a network or network device. Typically, threats are persistent due to vulnerabilities, which are problems that can arise as a result of poor hardware or software configuration, poor network design, inherited technology weaknesses, lack of training, or neglect of the final user.

2.5 El riesgo asumido se basa en el costo que se quiera tomar para salvaguardar la información. The security risks cannot be removed or prevented altogether; however, effective risk management and valuation can significantly minimize its existence. The risk assumed is based on the cost that is taken to safeguard the information.

2.6 The three main objectives of security seem very simple. However, the challenge of securing the network while taking operational needs into account can be a complex task. Administrators must carefully manage security policies to maintain the balance between transparent access, usage, and network security.

2.7 In relation to the above, and to the need for security external access, it is suggested:

1) To acquire networking equipment (routers firewall) for all nodes in order to:

   a) standardize the security equipment throughout the network,
   b) avoid unauthorized external and internal intrusions,
   c) address the lack of a border router in some nodes,
   d) management by the REDDIG II administrator of all firewalls (now subject to each state.

2) Implement a TACACS Server to control the accesses, create a community on the network computers to install a SISLOG (monitors all the events of the network, with the possibility of sending event information by mail), etc.

3) Define the assignment of user levels and keep a record on a server where all events will be hosted, which commands were executed, who entered, and so on.

4) Also, all of the above allows creating events for automatic backup when configuration changes are made to all networking computers.

2.8 It is extremely necessary to have a security plan to accurately define the architecture and operations, risks and security policies.

2.9 Subsequently, perform a joint analysis with the network personnel, to determine what type of events it is advisable to record (eg access to devices, changes in network interface status, hot restarts, changes in configuration parameters, etc.).

3. Firewalls

3.1 The most used application in recent years is the well-known firewall, a combination of hardware and software used by businesses and users to isolate the private network from abroad.

3.2 A firewall is a simple access control of the incoming / outgoing traffic of the user's network. In this control, the datagrams or packages that pass through it are reviewed and according to the rules imposed by the network administrator, will act accordingly: eliminating, forwarding or asking the administrator.

3.3 There are four types of firewalls: packet filtering, application level gateways, multilevel state inspection, and Circuit Level Gateways. The first two are the most used, but the multilevel inspection is the best considered. The big difference between them is the level of the OSI layer in which they work.

3.4 From the "Guide on Security Guidance for the Implementation of IP Networks" can be extracted:

3.4.1 Management must ensure adequate acquisition of the necessary resources for the protection of information, including network assets (routers, switches, etc.) and security (firewalls, IDS, IPS, etc.).

3.4.2 Each network must have a topology that takes into account the security aspects, considering at least the following:

a) Points of interconnection with other networks must have security assets, such as firewalls and IDS/IPS, installed and properly configured and monitored.

b) IP addresses should be designed so that they are not known on the Internet

c) Firewalls must be configured, at least, with the following rules:

- Deny all default policy;
- Web protocols (http, https, for example) only outgoing;
- E-mail protocols in both directions.

d) The routers must be configured considering the use of ACLs and NAT, as well as hiding the IP addresses.

e) Routers must be constantly updated, with different passwords and login from the factory.

f) The network interconnections with REDDIG II must be made with redundancy of assets, including those of security, and other measures that guarantee the availability and integrity of the information, as well as the performance of the network according to its specifications;

g) Connections with public networks (internet) must have a topology that guarantees security in multiple layers.

h) The network management must be done via the SNMP protocol version 3, with the activation of alerts and SNMP traps. Access to devices must be made using secure authentication;

i) Management links must be encrypted.

3.5 The Reference Guide constantly mentions the use of a firewall

4. Acquisition of firewalls routers for the whole network

4.1 The main objective is security, and in that sense the standardization and installation of networking equipment of the same characteristics will allow a greater robustness to the mitigation of vulnerabilities.

4.2 The administration of these equipments by the REDDIG II Administrator, and eventually the allowed access, with certain levels of privileges, to the different technicians that can intervene, will facilitate the control of accesses with good or bad intentions.

4.3 In this sense, the equipment required must have at least the following benefits:

1) A firewall as a combination of hardware and software used to isolate the private network from outside.

2) Allow reliable connections through proper firewall functions and access lists (ACLs).

3) Allow to configure NAT

4) Configuring Service Policies

5) Configuring access rules

6) Configuring AAA settings for access

7) Allow protocols inspection of each application layer

8) Provide information about the communications functions of the equipment

9) Allow the configuration of connection settings and quality of service (QoS)

10) Complex configurations for network protection.

11) Configuration of different modules.

5. Quantities and costs

5.1 In order to contemplate the installation of a firewall at all nodes and to have a backup, it is desirable to acquire 20 firewall equipment at an estimated value of around US$ 1000 to US$ 2000 each one. However, the value varies according to brand, model, license plates and licenses.

5.2 Take in consideration that equipment should be of a brand and supplier available in most States in order to be able to respond immediately to a contingency. Likewise, take in consideration the networking equipment that currently integrates the nodes of REDDIG II.
