International Civil Aviation Organization

Twenty Seventh Meeting of the Communications/ Navigation and Surveillance Sub-group (CNS SG/27) of APANPIRG

Bangkok, Thailand, 28 August – 01 September 2023

Agenda Item 9: Regional implementation review and updates

9.4 Contingency Planning for CNS/ATM Infrastructure

ACHIEVING HIGH RESILIENCE IN SUSTAINING OPERATIONS OF CRITICAL AERONAUTICAL INFRASTRUCTURE

(Presented by Hong Kong, China)

SUMMARY

Critical Aeronautical Infrastructure (CAI) needs uninterrupted operations for sustaining round-the-clock provision of air navigation services for flight safety purpose. This paper shares the experience of Hong Kong, China in the planning, design, implementation and maintenance of CAI in achieving high resilience in supporting its round-the-clock operations.

1. INTRODUCTION

1.1 CAI refers to an infrastructure that needs to maintain uninterrupted operations for sustaining round-the-clock provision of air navigation services for aircraft operating safely and efficiently within a Flight Information Region (FIR). It includes, but not limited to, air traffic control (ATC) centres, towers and corresponding equipment rooms, on-airport and off-airport communications, navigation and surveillance (CNS) stations, systems and supporting electrical and mechanical (E&M) facilities, such as power supply and air conditioning etc. Any degradation in performance of the systems and supporting E&M facilities of CAI may lead to disruption to its operations and even induce closure of the FIR as the last resort fail-safe measure. Resilience, redundancy and robustness (3R) are vital factors to consider in the planning, design and implementation of CAI for coping with unexpected emergency circumstances caused by natural disasters or human-induced incidents.

2. DISCUSSION

<u>ATC System Architecture & Design</u>

2.1 CAI in Hong Kong is designed and implemented with full considerations of "3R". From a system architecture perspective, the ATC systems are designed with multiple redundancies consisting of Main and Fallback systems. The Main and Fallback systems are identical systems operating in parallel that could provide immediate backup to each other when one system fails. For safety-critical ATC systems with serious consequence if failure, such as the air traffic management system, one additional layer of protection, namely a Contingency system completely independent from the Main and Fallback systems, is provided by another supplier for further enhancing resilience and mitigating the risk of total system breakdown due to simultaneous failure of Main and Fallback systems.

2.2 To ensure the Contingency system could function in full when the Main and Fallback systems fail simultaneously in the unlikely circumstances, same level of functionalities, capabilities and handling capacity as the Main and Fallback systems should be provided in the Contingency system in accordance with the guidance document developed by the "ICAO Asia/Pacific Air Traffic Management Automation System Task Force". To enable controllers to use the Contingency system more efficiently, it is beneficial to make the HMI and contents of data block display similar to Main/Fallback systems.

2.3 To eliminate the single-point-of-failure as far as practicable in hardware and software, all processing systems are interconnected via high capacity redundant local area networks (LANs). Computers providing core common services, such as Surveillance Data Processing Servers and Flight Data Processing Servers, are duplicated with each computer connected to each LAN providing a high degree of redundancy. The two individual LANs keep sharing information and function as main and fallback nodes. A third LAN is used for system logs collection and handling of recording and playback.

Location and Route Diversity

2.4 Location and route diversity are key considerations for robustness as it enables continuous operations even there are disruptions in one location or one communication cable routing. Key components of ATC systems, such as servers and core network switches, are installed at equipment rooms at different physical locations and interconnected via different cable routing such that ATC service would not be affected when one location or route experience disruption. In the Hong Kong International Airport (HKIA), there are multiple ATC centres/towers with identical systems provisions at different locations. In the event of unexpected emergency situation like fire or communicable disease (such as SARS, COVID pandemic) outbreak at one ATC centre or tower requiring evacuation, the backup ATC centre/tower at different locations could be activated within short duration so as to minimize impacts to ATC service. Similarly, fibre optics communication cables are installed in a ring configuration. When there is a failure in communication cables in certain route, relevant system information will be re-routed through another path. Regular activation drills of backup facilities are conducted to ensure readiness and familiarization by personnel involved.

City Mains Power & Gensets

2.5 The reliable provision of ATC service requires a highly resilient and robust power supply distribution network. The power utility company provides dual feeds with duty/backup transformers in a ring topology to ATC centres and towers at the HKIA, such that a breakage in the ring will not suspend power as illustrated in *Figure 1*. There are multiple gensets in "N+1" configuration with sufficient capacity for full ATC equipment loading inclusive of air conditioning to ensure provision of ATC service can be sustained by gensets only in case of prolonged city mains failure. Furthermore, the main switchboards are equipped with mobile genset plugin connection panels for quick hook-up to large-capacity mobile genset provided by either the power utility company or airport operator as shown in *Figure 2*. Again, regular activation drills of these mobile genset facilities are conducted to ensure readiness and familiarization by personnel involved.

Uninterruptible Power Supply (UPS)

2.6 All safety-critical ATC system servers installed at ATC centres/towers receive dual power inputs from two independent UPS sources. For ATC system workstations receiving only a single power source, static transfer switches connecting with two UPSes are put in place to provide UPS backup through automatic switching from one UPS source to another in case of failure/maintenance.

All UPSes are designed with capacity much higher than the total demand. Under extreme circumstances when power supply from both the power utility company and standby gensets is interrupted, UPSes can continuously support hours of uninterrupted operation of safety-critical ATC equipment, thus ATC service. *Figure 3* illustrates the UPS connections.

Air Conditioning

2.7 All safety-critical ATC servers/workstations and operational personnel are continuously and separately cooled by conditioned air to ensure their reliability and performance. In ATC centres, towers and corresponding equipment rooms, primary water-cooled chiller system of the central air conditioning system, with "N+1" redundancy in chillers and total capacity exceeding the full cooling load, operates round-the-clock to cool the ATC equipment and maintain a comfortable working environment for controllers in ATC centres/towers. In case of failure of all water-cooled chillers, which are extremely unlikely, the secondary air-cooled chiller system will kick in automatically to take up the cooling duty. Equipment rooms are equipped with computer room air conditioning units (CRAC) with duty and standby redundancy units.

2.8 For off-airport CNS stations, standalone air conditioners, such as split-type air conditioners, which possess duty and standby units, can alternately operate to serve the equipment rooms even under the maximum cooling loading. Remote monitoring and alert system is in place to ensure that any interruption in conditioned air supply will trigger the contingency plan for immediate resumption of conditioned air supply.

Comprehensive Maintenance

2.9 Apart from considerations of "3R" in the design and implementation of CAI, it cannot be stressed more that periodic drills (paper and on-load), system switchovers, routine, corrective and proactive maintenance, training and contingency plans are equally if not more important, for sustaining uninterrupted operations of CAI.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the experience of Hong Kong China in the planning, design, implementation and maintenance of Critical Aeronautical Infrastructure (CAI) in achieving high resilience in supporting its round-the-clock operations for flight safety purpose;

b) encourage CAAs/ANSPs to share their relevant experience;

c) consolidate the experience into a guidance document for future reference; and

d) discuss any relevant matter as appropriate.

– – – – – – – – – – – – –

Appendix

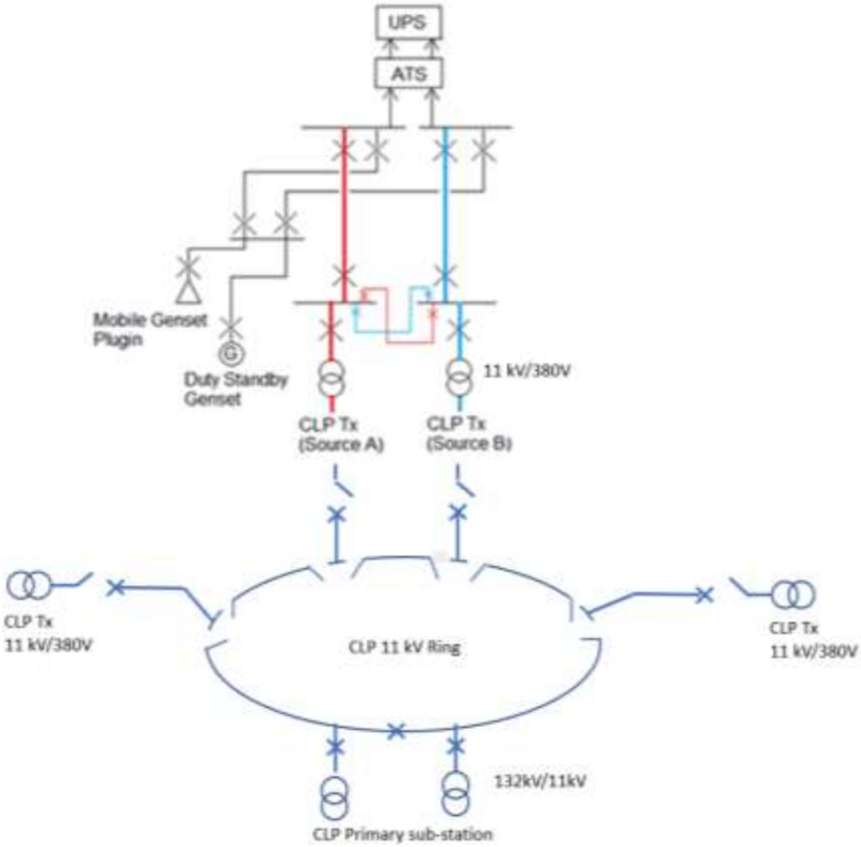

Figure 1 – Ring topology of dual power feeds by power utility company

Figure 2 – Mobile genset by power utility company

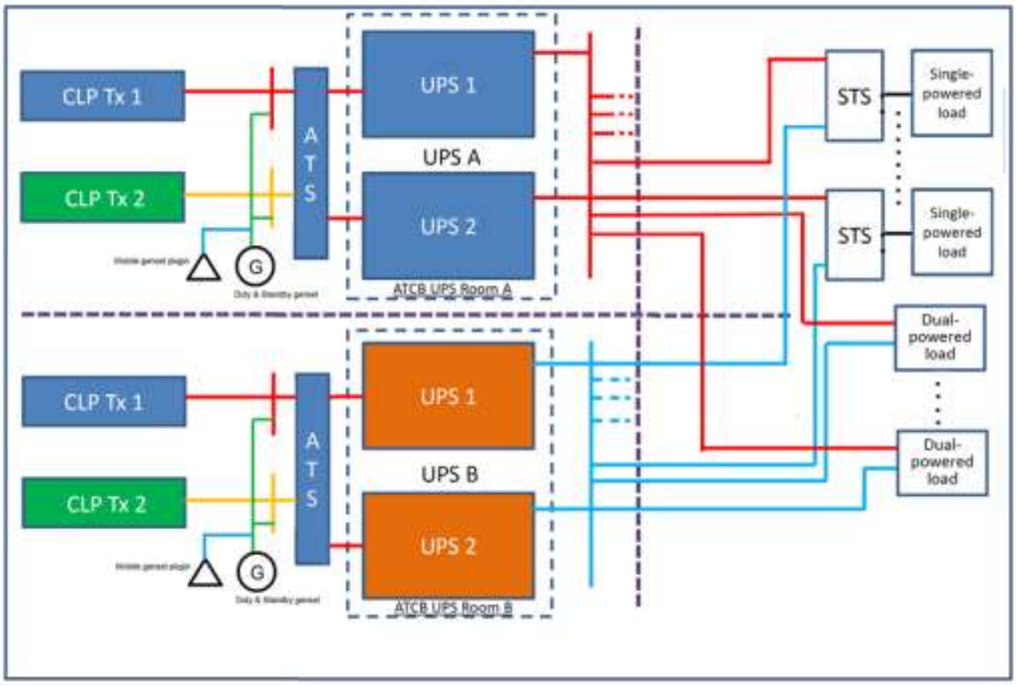

Figure 3 – UPS Connection Diagram