

Article

Algorithms of Cross-Domain Redundancy Management for Resilient of Dual-Priority Critical Communication Systems

Igor Kabashkin 

Engineering Faculty, Transport and Telecommunication Institute, Lauvas 2, LV-1019 Riga, Latvia; kiv@tsi.lv

Abstract: The paper presents models for managing cross-domain redundancy to enhance the reliability of two priority communication channels within critical infrastructure systems. Employing Markov chain models, the paper analyzes the impact of two distinct redundancy management strategies: a unified reserve pool and a separate pool approach with cross-domain resource sharing. The study introduces reliability improvement factors to quantify system performance, exploring their dependency on the number of additional redundant elements, their inherent reliability, and the chosen strategy for managing cross-domain redundancy. An air traffic control system serves as a case study of the application of the proposed management algorithms. Results indicate that the integration of resources from different priority domains significantly improves communication reliability. The findings may be useful for the design and operation of secure communication networks.

Keywords: algorithm for reserve management; multichannel communication; reliability; redundancy; Markov model

1. Introduction

Communication systems in high-security and mission-critical domains present unique challenges and requirements that set them apart from standard networks. These specialized areas, spanning aviation, military operations, emergency services, financial institutions, healthcare, nuclear facilities, space agencies, diplomatic corps, and critical infrastructure, all share a common need for robust, secure, and highly reliable communication channels. This reliability becomes even more essential in multi-channel communication systems, where the uninterrupted operation of high-priority channels is paramount, while lower-priority channels can tolerate some degree of communication loss.

Data centers and cloud computing services underpin much of today's digital infrastructure, operating multiple channels to serve diverse client needs [1]. Enterprise applications, especially those in the financial sector, require high-priority channels to ensure consistent uptime and reliability. These channels must be protected against any interruptions to maintain business continuity. Meanwhile, general consumer services operate on lower-priority channels, where occasional service disruptions are less impactful. By using resource reallocation, data centers can shift computational power and bandwidth from low-priority to high-priority channels during critical periods, thereby maintaining the necessary service levels for enterprise clients while managing overall resource efficiency.

Public safety and emergency services rely on robust multi-channel communication systems to coordinate their efforts effectively [2]. During emergencies, channels designated for police, fire, and medical services become a high priority, as any communication breakdown can impede response efforts and endanger lives. In contrast, municipal or public works communications are a lower priority and can afford some loss of connectivity. By temporarily reallocating communication resources from public works to emergency services during crises, these systems ensure that high-priority channels remain operational, facilitating efficient and effective emergency response.



Citation: Kabashkin, I. Algorithms of Cross-Domain Redundancy Management for Resilient of Dual-Priority Critical Communication Systems. *Algorithms* **2024**, *17*, 386. <https://doi.org/10.3390/a17090386>

Academic Editor: Costas Busch

Received: 29 July 2024

Revised: 25 August 2024

Accepted: 29 August 2024

Published: 2 September 2024



Copyright: © 2024 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Aviation communication systems are quintessentially multi-channel, catering to both civilian and military flights [3]. High-priority channels are used for military communications, handling classified and sensitive information that must remain secure and uninterrupted. Civilian communications, operating on lower-priority channels, manage routine flight operations. To ensure the reliability of high-priority channels, aviation systems employ cross-domain redundancy. When high-priority military channels face failures, civilian communication resources can be temporarily utilized to support military operations. Although this may reduce the availability of civilian channels, it ensures that critical military communications remain intact, reflecting a strategic balance to maintain overall system integrity.

The multi-channel nature of critical communication systems, coupled with their dual-priority structure, forms the backbone of many high-stakes operational environments. This architecture is not merely a technical choice but a strategic imperative that balances the need for uninterrupted, secure communication with practical operational realities. In these systems, the multi-channel approach serves as a fundamental reliability mechanism. By operating multiple independent channels, the system ensures that the failure of one channel does not compromise the entire communication network.

The dual-priority structure of these systems adds another layer of sophistication to their design. The high-priority domain, often referred to as the RED domain in secure communications parlance, handles critical, often classified information that must be protected at all costs. This domain is engineered with the highest levels of security and reliability, often featuring additional encryption, stricter access controls, and more robust infrastructure.

In contrast, the lower-priority domain, sometimes called the BLACK domain, handles less sensitive, often unclassified information. While still important, communications in this domain can tolerate brief interruptions or delays without catastrophic consequences. This tiered approach allows for more efficient resource allocation, focusing the most robust protections on the most critical information flows.

In normal operations, the domains remain strictly segregated, maintaining clear boundaries between sensitive and non-sensitive information. However, in emergencies or when resources are stretched thin, there is potential for controlled, secure sharing of resources between domains.

The reliability model for these systems must account for several key factors:

- The model needs to accurately represent the independence of multiple communication channels.
- The models of high-priority (RED) and lower-priority (BLACK) domains must account for cross-domain resource sharing in emergency situations.
- Reliability models must incorporate maintenance operations and repair times.
- Reliability models need to accurately represent how mechanisms of redundancy and failover mechanisms perform under various failure scenarios.

This paper aims to develop a comprehensive reliability model for advanced communication systems that operate with multiple channels and distinct priority levels. To ground this theoretical work in practical reality, we will use air traffic control (ATC) communication systems as our primary case study. Air traffic control serves as an excellent example for our modeling efforts due to its critical nature and complex operational requirements. While our focus is on air traffic control, the principles underlying this model can be applicable to other critical communication systems that share similar characteristics.

The remainder of this paper is structured as follows. Section 2 provides a review of the current literature in the field of two priority communication systems with RED/BLACK architectures. Section 3 introduces the concepts and methodologies employed in the study, describing in detail the architecture of RED/BLACK communication systems, discussing the reliability issues inherent in these architectures, and introducing the concept of cross-domain redundancy for enhancing their reliability. Section 4 presents two distinct algorithms for managing cross-domain redundancy in RED/BLACK systems and provides detailed Markov chain models for each approach. Mathematical expressions for

steady-state probabilities and channel availability are derived for both strategies. Section 5 discusses the results. It compares the performance of the two proposed algorithms and examines the reliability improvement achieved through cross-domain redundancy. This Section includes a detailed interpretation of the graphical results, exploring the implications of varying system parameters on overall reliability. Section 6 summarizes the key findings of the study, discusses their implications for the design and operation of critical communication systems, and suggests directions for future research in this field.

2. Related Works

The exploration of reliability in communication systems within the scope of the RED/BLACK equipment domains, intersects various fields, including aviation communication, information security, and reliability engineering. This Section reviews relevant research that contributes to the foundation and context of this study.

Issues of reliability of ATC are very important for the safety of flights. The chapter [4] describes a system for air traffic management (ATM), designed to manage multiple flight trajectories simultaneously for safe and efficient air traffic flow. The paper [5] addresses the challenges of data exchange in the ATM system, particularly as air traffic volumes increase, impacting the interoperability between the ATM system and its data sources. The study [6] introduces a comprehensive model to assess air traffic network reliability, considering connectivity, travel time, and capacity aspects. Applying this model to the air traffic network reveals a reliable system, identifying key operational strengths and areas for improvement, which is valuable for future traffic planning and management.

The novel semantic-based searchable encryption scheme for enhancing data security in the aviation industry, addressing the vulnerability of unencrypted aircraft communications and flight data is introduced in [7]. The proposed solution, rigorously analyzed for security and efficiency, is effective for text-level encryption and is tested with a real-world aviation dataset, demonstrating its potential for secure, privacy-preserving, and lightweight data protection against distinguishability attacks in the aviation sector.

The study [8] examines the security vulnerabilities in aviation communication systems, particularly the controller–pilot data link communications (CPDLC), in the face of increasing hacking risks. It assesses CPDLC's technological aspects to construct a threat model and suggests several solutions for enhancing the security of data messaging in ATM. The paper explores the potential of elliptical curve cryptography, protected aircraft communications addressing and reporting systems, and the Host Identity Protocol as countermeasures. Additionally, it evaluates identity-defined networking as a comprehensive security solution that would necessitate global changes in air traffic communication systems.

The paper [9] addresses the security vulnerabilities in automatic dependent surveillance–broadcast (ADS-B) data transmission within communications, navigation, and surveillance/air traffic management (CNS/ATM) systems. It proposes a security framework that employs simple public key infrastructure certificates for ADS-B sensor authorization and symmetric cryptography for encrypting data between ADS-B sensors and ATC. This framework includes an ADS-B sensor authentication module, an encrypted data processing module, and an ADS-B sensor information management module. By implementing this framework, the CNS/ATM system can effectively counter security threats like ground station flood denial, ghost injection, and data modification.

Mission-critical communications of ATM are discussed in [10]. The paper outlines the increasing risks of communication failure in busier airports and complex ATM environments. It emphasizes the importance of real-time, deterministic CNS/ATM information transmission for aircraft safety and operational efficiency.

The optimization of radio resources in aviation has been the subject of numerous studies. The study [11] addresses enhancing reliability in ATM communication systems by proposing a dynamic distribution of communication equipment across channels. It contrasts this approach with traditional redundancy methods, using a mathematical model for channel reliability and comparative analysis in real ATM conditions.

The report [12] outlines the development and evaluation of a prototype internet protocol-based voice communication system for ATC, designed to connect controllers with pilots via radio. The role of redundancy and maintenance in secure communication systems is critical, as explored in [13]. This paper explores the enhancement of communication channel reliability in ATC systems, which are crucial for flight safety. It focuses on the effectiveness of using redundancy with a common set of standby radio stations, combined with periodic maintenance, to improve communication between air traffic controllers and pilots.

The origins and applications of the RED/BLACK concept have not been extensively discussed in the literature. Both the concept itself and the equipment that implements it are reflected mainly only in information from manufacturers of such equipment. The voice communication systems include important features to cope with the specific needs of advanced and secure communications on the basis of the RED/BLACK concept, which are described in [14]. Red/Black Web-Based HF Radio system monitoring is described in [15]. In [16] the RED/BLACK multi-level security architecture for secure and non-secure communications is given.

L3Harris has developed a digital inter-communication system (ICS) that provides operators with intuitive and flexible access to mission audio. The ICS-based platforms can use their red/black separation features for simultaneous and secure audio [17]. The VOICE C2 Red/Black [18] is a system, tailored for secure, multi-enclave operations in fixed and deployable air defense settings. The system allows simultaneous access to both secure (RED) and non-secure (BLACK) communication channels, integrating operator positions, communication equipment, and a cross-domain solution for unified control of both asset types from a single console.

The R&S[®] M4ACS is a state-of-the-art, fully IP-based voice communications system designed for seamless airspace operations, combining rich functionality with exceptional usability [19]. Using the benefits of IP technology, it offers robust security, resilience, and supports crypto pooling. It enables operators to manage all communications from a single screen while maintaining strict security. The system distinctly separates secure (RED) and unsecure (BLACK) domains, allowing simultaneous access to both using the same audio accessories.

AviCom is an advanced radio and audio management system designed to give aircraft crews complete control over communication assets, ensuring secure audio management [20]. It digitally processes audio, classifying it as secure (RED) or non-secure (BLACK), with hardware-level interlocks guaranteeing the protection of secure communications. This system is adaptable for various RED security levels, making it suitable for clients with complex national and international security needs on a unified platform.

Orion's RED/BLACK switch facilitates a seamless shift from unsecured to highly secure communications, integrating with radio encryption terminals [21]. This device enables the placement of encryption mechanisms in a secure zone, distinct from radio equipment, accommodating operational scenarios that require the separation of encrypted digital radio packets and secure voice calls.

Radio communications reliability issues are one of the key components of the air traffic control system. The paper [22] discusses the advent of cognitive radio technology, highlighting its prospects for enhancing spectrum efficiency in civil aviation by enabling dynamic spectrum access. It delves into the current research, regulatory landscapes, and the challenges hindering its adoption in aviation.

The paper [23] examines how advancements in power electronics and energy processing can potentially disrupt onboard aircraft equipment and ground stations that provide air traffic services, with a specific focus on emergency radio systems. It details experimental efforts to measure the effects of high-power electronic interference on emergency radio systems, highlighting the significant risks posed to aircraft backup systems and very high-frequency radios.

The rapid advancement of remotely piloted aircraft systems in commercial and research sectors, noting the challenges of integrating these services into non-segregated civilian airspace, including regulatory, security, and technical issues, is discussed in paper [24]. The paper introduces a flexible communication infrastructure manager utilizing software-defined networking and virtualization to manage this complexity and meet regulatory demands for communications.

The role of air traffic control automation systems in managing flight order and ensuring aviation safety is discussed in [25]. It emphasizes the importance of reliability prediction during the ATC system design phase and safety evaluation during operation. The focus of the research is on developing models for both reliability prediction and safety evaluation tailored to the general architecture of ATC systems.

The paper [26] highlights the crucial issues of communication errors in civil aviation safety and management. It proposes the implementation of a supervisory control and data acquisition system for ATM. This centralized system would facilitate information exchange and aid management systems in making informed decisions for ATM.

The factors impacting the operational reliability of ATC communication systems, proposing concepts, and methodologies tailored to the unique characteristics of the ATC communication network are analyzed in [27]. Using the civil aviation communication network as an example, it examines the development of backup systems, evaluation methods, and ideas for reliability management within these critical communication frameworks.

The report [28] addresses the limitations of current broadcast radio communication in air traffic control, noting that a significant portion of such communication is dedicated to the procedural complexity of transferring aircraft between sectors. It posits that digital end-to-end communication, akin to mobile technology, will eventually supplant current methods, offering substantial benefits by rendering the internal air traffic control structure transparent to aircrews, with systems automatically connecting aircraft to the appropriate controller. The paper explores the challenges and advantages of this shift and suggests adaptations to existing broadcast standards to simulate an end-to-end communication system in the interim.

The integration of sophisticated automatic speech recognition technologies in ATC is discussed in [29]. The paper describes an algorithm to convert speech into ontology instructions and outlines an interface for reliable ATC communication, which accounts for plausibility values, speaker identification, and ambiguous outputs.

The report [30] discusses the development and evaluation of a prototypical IP-based voice communication system for air traffic control, designed to connect controllers with pilots via radio. This system integrates telephone and radio services, records communications, and allows retransmission across multiple channels, with the prototype enabling simultaneous connection for two users. The project also tested system latency, revealing inconsistencies in measurement methods, and emphasizing the need for careful selection and application of these methods.

The literature reviewed underscores the complexity of maintaining reliability in secure communication systems and emphasizes the continuous need for improvement in their management and operation. However, the gap in the literature becomes apparent when considering the dynamic nature of communications redundancy in air traffic management systems and the specific application of cross-domain resource allocation for enhancing reliability.

This paper aims to bridge this gap by providing a comprehensive Markov reliability model for multichannel communication systems. It extends beyond the foundational approaches identified in the literature by offering a granular analysis of system behavior under various operational conditions and resource management strategies, which have not been as thoroughly examined in previous studies.

3. Materials and Methods

3.1. RED/BLACK Concept of Communication in Aviation

The RED/BLACK concept represents a fundamental framework in secure communications, underpinning the design of mission-critical systems. This concept delineates sensitive classified RED domains from non-sensitive unclassified BLACK domains, enabling the simultaneous transmission and processing of both open and restricted information flows.

In aviation systems, for example, the RED designation refers specifically to communication networks, equipment, protocols, and data authorized to handle confidential, secret, or top-secret information. This encompasses systems that transmit encrypted communications vital for military, law enforcement, or other operations pertinent to national security. Conversely, the BLACK designation refers to standard commercial systems for public aviation communication and air traffic control operations involving routine non-sensitive information.

The segregation between RED and BLACK ensures that sensitive information remains isolated and uncompromised while allowing regular aviation communication to occur freely across the BLACK domain. This bifurcation is physically manifested through separate infrastructure for both domains including distinct radio systems, antennas, networks, storage systems, and facilities restricting access only to personnel with appropriate security clearances for the RED domain.

The segregation also encompasses stringent security protocols enveloping all aspects of RED communications, ensuring confidentiality and integrity. These include encryption mechanisms, access control and monitoring systems, robust physical security measures, and extensive personnel vetting procedures aligned to the level of information sensitivity.

The main applications of the RED/BLACK concept are shown in Table 1.

Table 1. The main functions and applications of the RED/BLACK concept.

Applications of RED/BLACK Concept	Description
RED Communications	- These are the channels or systems that handle classified, sensitive, and secure communications. - Information transmitted via RED radios is often encrypted and requires authorized access. - The equipment and wiring used for RED communications are designed to prevent any form of electronic eavesdropping or interception. - RED communications must be processed, stored, and transmitted using secure methods that meet stringent government and military standards.
BLACK Communications	- These involve non-classified, public, or less sensitive information that does not require the same level of security as RED communications. - BLACK radios can include routine air traffic control communications with aircraft, where the information does not have implications for national security. - The systems and networks for BLACK communications are typically not encrypted or are encrypted at a lower level of security.
Separation	- The separation is both physical and electronic. Physically, the equipment might be color-coded, with RED cables and devices clearly marked to avoid accidental cross-connections with BLACK systems. - Electronically, the systems are designed so that RED and BLACK signals are processed through separate circuits and can never intersect. This prevents any potential leakage of classified information into unclassified channels.
Implementation in Air Traffic Control	- In air traffic control, the concept would be applied by using separate radio systems for RED and BLACK communications. The RED radios might be used for secure military communications or other sensitive information exchanges, while the BLACK radios would handle the routine management of civilian air traffic. - Air traffic control centers that manage both civilian and military aircraft, or those located near sensitive installations or borders, might require such a system to ensure the security of communications.

Table 1. Cont.

Applications of RED/BLACK Concept	Description
Security Protocols	- The RED/BLACK concept is supported by strict protocols and procedures. Personnel are trained to understand the importance of the separation and to handle each type of information appropriately. - Regular security audits and checks are conducted to ensure that the separation is maintained and that no cross-contamination occurs between RED and BLACK systems.

3.2. Architecture of RED/BLACK Communication

The architecture that physically realizes RED/BLACK communications encompasses specialized infrastructure and protocols aligned to securely segregate sensitive and public data functions in aviation systems. The foundation lies in physical separation through dedicated RED and BLACK hardware—distinct sets of radios, antennas, cabling, routing equipment, and control systems provisioned for each domain. It is important that the terminal devices—radio stations—are identical in both domains and differ only in tuning frequencies.

Network architectures implement logical controls and monitoring systems to sustain electronic separation. RED networks are further hardened through encryption, access restrictions, and data leakage countermeasures integrated through secure gateways for external interfaces. BLACK networks leverage standard cybersecurity protections.

A hallmark of the RED/BLACK environment is sustained redundancy within each domain ensuring maximum information assurance. RED systems mandate comprehensive redundancy with dedicated failover infrastructure guaranteeing near-continuous functionality. BLACK implements cost-optimized redundancy suiting commercial reliability parameters.

The specified architecture, divided into two domains, creates high security for the operation of the RED domain, but at the same time requires a certain redundancy due to the allocation of communication resources, which generally reduces the efficiency of the use of communication equipment.

3.3. Reliability Issues of RED/BLACK Architecture

While the RED/BLACK bifurcation provides crucial security assurances, the isolated nature of the domains introduces inherent reliability challenges for such systems. Strict physical and logical separation creates confined silos, limiting collective redundancy strengths compared to integrated systems.

Isolating the high-assurance RED environment incurs overheads, directly impacting service availability and mean time between failures compared to the relatively open BLACK domain. Obtaining like-for-like RED and BLACK redundancy entails proportionally high costs due to stringent RED assurance needs. Robust partitioning also restricts shared fate resilience offered through loosely coupled architectures.

These reliability differentials must be carefully evaluated when considering innovations like the cross-domain resource sharing proposed in this paper. The architecture must balance reliability gains from added redundancy against the risks of improperly segregating RED and BLACK environments when resources are mixed. A reliability model mapping domain interdependencies could help assess these factors.

3.4. Redundancy of Hardware in the Architecture of RED/BLACK Communication

Redundancy is pivotal in the RED/BLACK architecture to assure the continuity and integrity of sensitive classified environments alongside the availability of routine aviation communications. Redundancy in aviation communication systems is not just a measure of reliability; it is a necessity for safety and security. The critical nature of these communications requires that there is no single point of failure. Both the RED (secure) and BLACK

(non-secure) domains must maintain continuous operation, as any disruption could have serious implications.

Continuous monitoring systems of RED/BLACK architecture are implemented to detect failures or degradations in system performance. Upon detection of a failure, automated systems switch operations to the redundant systems without manual intervention, ensuring minimal disruption. RED requires failover mechanisms to handle fast security key rotations alongside equipment switchovers. BLACK leverages standards-based redundancy protocols. Blending standards where feasible improves cost efficiencies without diluting security capabilities.

3.5. Cross-Domain Redundancy for Reliable ATM Communication with RED/BLACK Domains

The typical architecture of air traffic management communication with RED/BLACK domains is shown in Figure 1, focusing on the segregation between RED and BLACK domains. In this context, “RED” would represent secure, sensitive, or classified networks, while “BLACK” refers to unclassified or less secure networks.

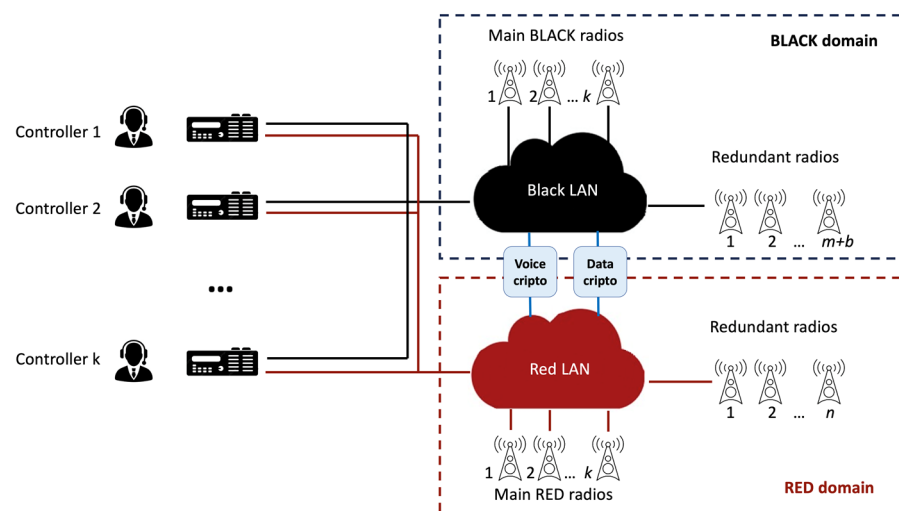


Figure 1. Architecture of air traffic management communication with RED/BLACK domains.

There are two separate local area networks (LAN), one marked in black and the other in red, indicating the unclassified and classified domains, respectively. Each domain has its own set of local radios and remote radios, with the classified domain’s elements marked in red, and the unclassified in black. The controller manages the interactions between these two domains.

The two domains are kept separate to ensure that classified information remains secure and that there are clear distinctions between the types of information transmitted or received across these networks.

The robustness of ATM systems is a critical factor in ensuring the safety of air navigation. A lapse in the efficacy of communication between air traffic controllers and pilots is not just problematic but potentially hazardous as a significant contributor to aviation accidents. The ATM system employs a variety of air traffic controllers—tower, approach, and departure, and route controllers—each reliant on independent communication channels operating at specific radio frequencies. These frequencies facilitate the uninterrupted interaction with aircraft across different phases of flight.

In the complex environment of air traffic control centers, the communication network is dual-layered, comprising RED and BLACK domains to handle secure and non-secure information, respectively. Each air traffic controller is supported by two independent sets of radio stations (RS). The local set is within the air traffic control center for immediate access, while the remote set, consisting of more powerful RS, is typically housed at a distance located, as a rule, several kilometers from the airport, within a remote radio center. In this

case, the approach to ensuring the reliability of each of the radio centers, local and remote, is implemented in the same way, which allows them to be considered independently on the basis of the same model.

The most effective method for increased reliability of communication in ATC multi-channel systems is to use $N = k + n$ RS, where k is the number of ATM channels provided by a similar number of main radio stations (MRS) and n denotes a set of universal standby radios [31]. The voice communication system is the core component of this architecture, facilitating all necessary switching operations and frequency restructuring within the reserve.

For RED domain controllers, who carry out highly responsible missions, it is imperative to ensure even greater reliability of their communication channels. One of the approaches to bolstering this reliability is the strategic utilization of the BLACK domain resources in contingency scenarios. If all backup RS in the RED domain were to fail, a pre-determined number of RS from the BLACK domain could be requisitioned as an additional reserve for domain RED.

The reliability enhancement from this method is multi-fold. First, it provides an extra layer of fail-safes beyond the conventional redundancy already in place. Second, it introduces a level of flexibility in resource allocation that is uncommon in standard communication system designs. Third, the approach optimizes the utilization of available resources, effectively increasing the operational resilience of the system without necessitating the procurement of additional dedicated hardware.

This paper aims to analyze the degree to which this innovative redundancy strategy improves the reliability of RED domain communication channels (CC). The study provides insights into the effectiveness of integrating BLACK domain resources as an additional redundancy layer for the RED domain in communication systems from the RED domain CC reliability point of view.

4. Results

In this Section, we introduce two strategic approaches for managing cross-domain redundancy in RED/BLACK communication systems. These approaches, referred to as ‘strategies’ throughout the Section, involve specific rules and methodologies for allocating and managing redundant resources across the RED and BLACK domains. Rather than procedural algorithms in the traditional sense, these strategies represent high-level frameworks that guide the redundancy management process. Their effectiveness is analyzed through Markov chain models, which allow us to evaluate the reliability improvements they offer.

4.1. Algorithms for Managing Cross-Domain Redundancy in RED/BLACK Systems

There are two algorithms for managing cross-domain redundancy in RED/BLACK communication systems with two distinct strategies that offer different approaches to resource allocation and system resilience.

The first algorithm proposes a unified reserve pool that combines resources from both RED and BLACK domains. This integrated approach allows for dynamic allocation of reserve resources across domains as needed. Under this model, when a failure occurs in either domain, the system can draw from the combined pool of reserve radio stations, regardless of their original domain designation.

The advantages of this unified approach include the following:

- Improved resource efficiency, as all reserve units are available to both domains.
- Potentially faster response to failures, as there’s no need to exhaust one domain’s resources before accessing the other.

The second algorithm proposes a more conservative, staged approach to cross-domain redundancy. In this model, each domain (RED and BLACK) initially operates with its own dedicated reserve pool. The RED domain, being a higher priority, gains access to BLACK domain resources only after exhausting its own reserves. This approach maintains a stricter separation between domains under normal operating conditions.

Advantages of this staged approach include the following:

- Clearer security boundaries between domains during normal operations.
- Simplified resource management within each domain.

Both algorithms offer unique trade-offs between security, efficiency, and complexity. The choice between them would depend on specific operational requirements, security policies, and risk tolerance of the critical infrastructure system.

Our analysis focuses on quantifying the reliability improvements offered by each strategy compared to systems without cross-domain redundancy. The following results present the comparative performance of these models under various operational scenarios and system configurations.

To analyze algorithms for managing cross-domain redundancy in RED/BLACK communication systems, we will use the Markov chain models. The Markov model, with its memoryless property, is particularly suited for analyzing communication systems because it can model the probabilities of failures and recoveries based on the current state of the system without the need for historical data. For example, if a communication channel within the RED domain is in a ‘degraded’ state, the Markov model can predict the likelihood of it failing completely or recovering to full functionality in the next time step.

This probabilistic analysis provided by the Markov chain allows us to identify weak points in the communication architecture and to design redundancies and safeguards that can improve the overall reliability of the RED domain. By simulating various scenarios through the Markov model, we can anticipate the behavior of the communication channels during different operational conditions and can implement strategic improvements.

Furthermore, the Markov model can bridge the gap between theoretical resilience and practical performance. It provides a quantitative framework that can inform the development of protocols and technologies to bolster the security and reliability of the RED domain, ensuring that classified information remains protected while maintaining the continuous flow of communication necessary for effective operations. In this case, the Markov model serves as an important tool in the risk management and optimization of secure communication channels within the RED/BLACK domains.

The reliability analysis presented in this study focuses on steady-state reliability, which pertains to the long-term behavior of the system once it has reached a regime condition. Steady-state analysis is particularly useful for evaluating the long-term availability and reliability of systems, which is critical for dual-priority communication systems where continuous and reliable operation is paramount. The assumption of steady-state conditions allows us to concentrate on the system’s performance after transient effects have dissipated, providing a clearer picture of its reliability under normal operating conditions.

The following symbols have been used to develop equations for the models:

λ —failure rate for MRS and RRS;

μ —repair rate for MRS and RRS;

$\gamma = \lambda/\mu$ —reliability parameter;

k —number of communication channels and MRS in the RED domain;

n —number of RRS in the RED domain;

$N = k + n$ —total number of RS in the RED domain;

h —number of communication channels and MRS in the BLACK domain;

m —number of RS allocated in the BLACK domain for possible additional reservation of RS in the RED domain;

$M = h + m$ —total number of RS in the RED domain;

A_R —channel availability in the RED domain with traditional architecture;

A_{RD} —channel availability in the RED domain with cross-domain RS redundancy from the BLACK domain;

$U_R = 1 - A_R$ —channel unavailability in the RED domain with traditional architecture;

$U_{RD} = 1 - A_{RD}$ —channel unavailability in the RED domain with cross-domain RS redundancy from the BLACK domain;

p_i —stationary probability of the state H_i in Markov model.

The models were built for the case of restoring failures by one repair unit in each domain. All switching of radio stations in the system is assumed to be automatic and instantaneous, and the switching devices themselves are assumed to be fail-free.

4.2. Model for Algorithm with Unified Pool of Reserve Resources of RED/BLACK Domains

The operation of the discussed system is described by the Markov Chain state transition diagram (Figure 2), where H_0 —initial state of fully reliable equipment without failures; H_i —state in which i RS failed, but the dedicated channel has available RS; H_{if} —state of the system in which $i + 1$ RS are failed RS, including radios in the dedicated communication channel.

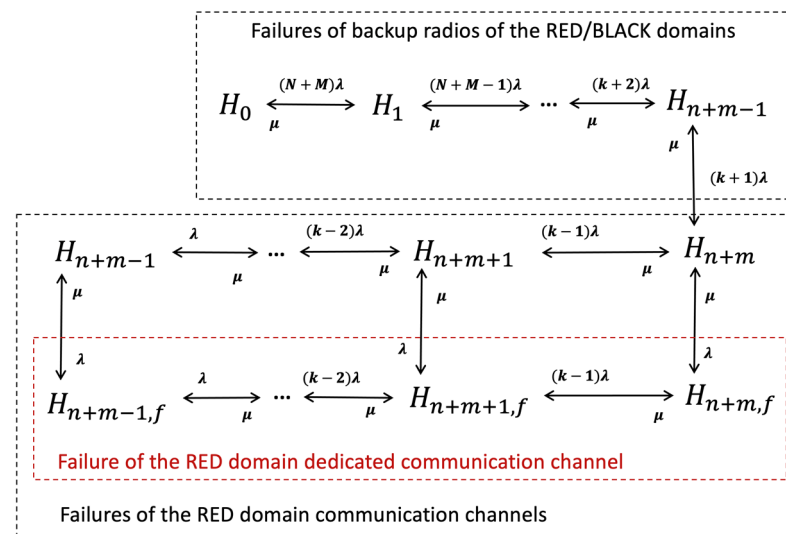


Figure 2. Markov model for the algorithm with a unified pool of reserve resources of RED/BLACK domains.

In accordance with the diagram (Figure 3), the system of Chapman–Kolmogorov’s equations can be written on the basis of the general rules [32] directly from the Markov Chain state transition diagram:

$$p_i = \frac{(N+M)!}{(N+M-i)!} \gamma^i p_0, \quad 1 \leq i \leq n+m$$

$$p_{n+m+i} = \frac{(N+M)!}{(k+h)!(k-i-1)!k} \gamma^{n+m+i} p_0, \quad 0 \leq i \leq k-1$$

$$p_{n+m+i,f} = \frac{(N+M)!(i+1)}{(k+h)!(k-i-1)!k} \gamma^{n+m+i+1} p_0, \quad 0 \leq i \leq k-1$$

The normalizing condition is:

$$\sum_{\forall i} p_i(t) = 1 \quad (1)$$

Value of p_0 can be obtained by replacement $p_i, \forall i$ and $p_{i,f}, \forall i$ in the normalizing Equation (1):

$$p_0^{-1} = (N+M)! \left\{ \sum_{i=1}^{n+m} \frac{\gamma^i}{(N+M-i)!} + \frac{\gamma^{n+m}}{k(k+h)!} \left[\sum_{i=1}^{k-1} \frac{1}{(k-i-1)!} \gamma^i + \sum_{i=0}^{k-1} \frac{i+1}{(k-i-1)!} \gamma^{i+1} \right] \right\}$$

On the base of the obtained equations of probabilities for the algorithm with a unified pool of reserve resources of RED/BLACK domains, the channel availability in the RED domain is obtained as

$$A_{RD1} = 1 - U_{RD} = 1 - \sum_{\forall i,f} P_{if} = \frac{a_1 + a_2}{a_1 + a_2 + a_3}, \quad (2)$$

where

$$\begin{aligned} a_1 &= (N + M)! \left(\sum_{i=1}^{n+m} \frac{\gamma^i}{(N + M - i)!} \right) \\ a_2 &= \frac{(N + M)! \gamma^{n+m}}{k(k+h)!} \sum_{i=0}^{k-1} \frac{(k-i)!}{(k-i-1)!} \gamma^i \\ a_3 &= \frac{(N + M)! \gamma^{n+m}}{k(k+h)!} \sum_{i=0}^{k-1} \frac{(i+1) \gamma^{i+1}}{(k-i-1)!} \end{aligned}$$

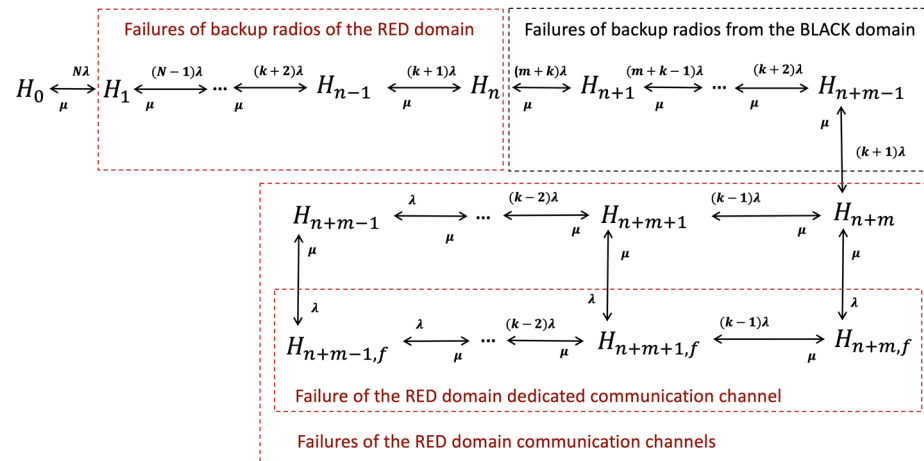


Figure 3. Markov model for algorithm with separate reserve pools of reserve resources of RED/BLACK domains.

4.3. Model for Algorithm with Separate Reserve Pools of Reserve Resources of RED/BLACK Domains

The operation of the discussed system is described by the Markov Chain state transition diagram (Figure 3), where H_0 —initial state of fully reliable equipment without failures; H_i —state in which i RS failed, but the dedicated channel has available RS; H_{if} —state of the system in which $i + 1$ RS are failed RS, including radios in the dedicated communication channel.

In accordance with the diagram (Figure 3), the system of Chapman–Kolmogorov’s equations can be written on the basis of the general rules [32] directly from the Markov Chain state transition diagram:

$$\begin{aligned} p_i &= \frac{N!}{(N-i)!} \gamma^i p_0, \quad 1 \leq i \leq n \\ p_{n+i} &= \frac{N!(m+k)!}{(N-i)!(m+k-i)!} \gamma^{n+i} p_0, \quad 1 \leq i \leq m-1 \\ p_{n+m+i} &= \frac{N!(m+k)!}{(k-i-1)!k} \gamma^{n+m+i} p_0, \quad 0 \leq i \leq k-1 \\ p_{n+m+i,f} &= \frac{N!(m+k)!(i+1)}{(k-i-1)!k} \gamma^{n+m+i+1} p_0, \quad 0 \leq i \leq k-1 \end{aligned}$$

Value of p_0 can be obtained by replacement p_i , $\forall i$ and $p_{i,f}$, $\forall i$ in the normalizing Equation (1):

$$p_0^{-1} = N! \left[\sum_{i=1}^n \frac{\gamma^i}{(N-i)!} + \sum_{i=1}^{m-1} \frac{(m+k)!}{(N-i)!(m+k-i)!} \gamma^{n+i} \right] + \frac{N!(m+k)! \gamma^{n+m}}{k} \left[\sum_{i=1}^{k-1} \frac{\gamma^i}{(k-i-1)!} + \sum_{i=0}^{k-1} \frac{(i+1) \gamma^{i+1}}{(k-i-1)!} \right]$$

On the basis of the obtained equations of probabilities, the channel availability in the RED domain for the algorithm with separate reserve pools of reserve resources of RED/BLACK domains is obtained as

$$A_{RD2} = 1 - U_{RD} = 1 - \sum_{i,f} p_{i,f} = \frac{a_1 + a_2}{a_1 + a_2 + a_3}, \quad (3)$$

where

$$a_1 = N! \left[\sum_{i=1}^N \frac{\gamma^i}{(N-i)!} + \sum_{i=1}^{m-1} \frac{(m+k)! \gamma^{n+i}}{(N-i)!(m+k-i)!} \right]$$

$$a_2 = \frac{N!}{k} \sum_{i=0}^{k-1} \frac{\gamma^{n+m+i}}{(k-i-1)!}$$

$$a_3 = \frac{N!}{k} \sum_{i=0}^{k-1} \frac{(i+1) \gamma^{n+m+i+1}}{(k-i-1)!}$$

5. Discussion

The analysis of two distinct algorithms for managing cross-domain redundancy in RED/BLACK communication systems reveals important insights into the reliability and efficiency of these critical infrastructure systems. Our results demonstrate that both cross-domain redundancy strategies offer significant improvements in reliability compared to traditional isolated architectures. However, the comparative performance between the two algorithms reveals nuanced trade-offs between resource efficiency, operational complexity, and security considerations.

While the term “algorithm” is used to describe these strategies, it is important to note that these are conceptual frameworks rather than computational procedures. The analysis presented focuses on the theoretical evaluation of these strategies through Markov chain modeling, providing insights into how they can enhance system reliability. Future work could involve the development of more detailed procedural algorithms that implement these strategies in practical applications, offering step-by-step guidelines for their deployment in real-world systems.

Figure 4 illustrates the relative performance of the two algorithms by showing the reliability improvement factor B as a function of the number of reserve elements in both the RED (n) and BLACK (m) domains for a system with the number of channels $h = 8$ in the BLACK domain and $k = 10$ in the RED domain. This factor B represents the ratio of unavailability between the unified pool algorithm (A_{RD1}) and the separate pools algorithm (A_{RD2}), effectively quantifying how much more reliable the separate pools approach is compared to the unified pool approach:

$$B = \frac{1 - A_{RD1}}{1 - A_{RD2}} = \frac{U_{RD1}}{U_{RD2}}$$

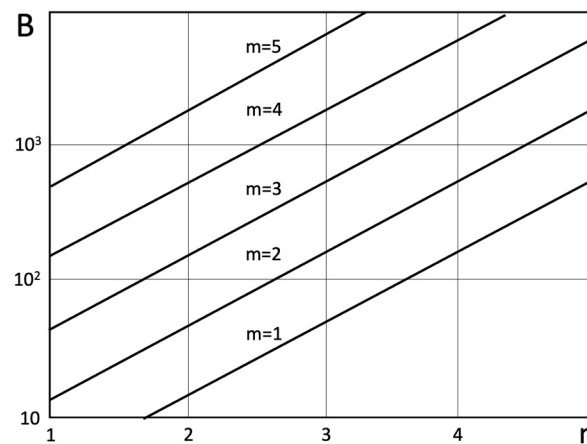


Figure 4. Factor of reliability improvement for strategy of cross-domain redundancy with the first algorithm of reserve resources management compared with the first one.

The graph in Figure 4 depicts several key insights:

- The reliability improvement factor B generally increases as the number of reserve elements in both domains increases, indicating that the separate pools algorithm becomes increasingly advantageous as more backup resources are available.
- The improvement is showing diminishing returns as the number of reserve elements grows, particularly in the RED domain.
- The impact of increasing reserve elements in the BLACK domain (m) appears more pronounced than increasing reserves in the RED domain (n), especially when n is small. This suggests that leveraging BLACK domain resources can be particularly effective for improving RED domain reliability.
- There are noticeable “steps” in the improvement factor, particularly visible as m increases.
- The complex interplay between RED and BLACK domain reserves emphasizes the importance of considering both domains holistically when designing redundancy strategies.

This visualization underscores the potential benefits of the separate algorithm, particularly in scenarios where a high number of reserve elements can be allocated in both domains. However, it also hints at the need for careful optimization, as the gains from additional reserves are not uniform and may need to be balanced against increased system complexity and cost.

To quantify the reliability improvement achieved by the second strategy (separate pools with cross-domain access) compared to the classical approach (RED domain using only its own reserves), we introduce the factor of channel availability improvement V :

$$V = \frac{1 - A_R}{1 - A_{RD2}} = \frac{U_R}{U_{RD2}}$$

where A_R represents the availability of the system with only RED domain reserves (classical approach), and A_{RD2} is the availability of the system using the second strategy with cross-domain redundancy. The value of A_{RD2} is determined using Equation (2), while A_R was derived in previous studies [33].

Figure 5 illustrates the reliability improvement factor V as a function of the additional standby radio stations m in the BLACK domain that can be accessed by the RED domain. The graph shows multiple curves, each representing a different reliability parameter γ of the radio stations.

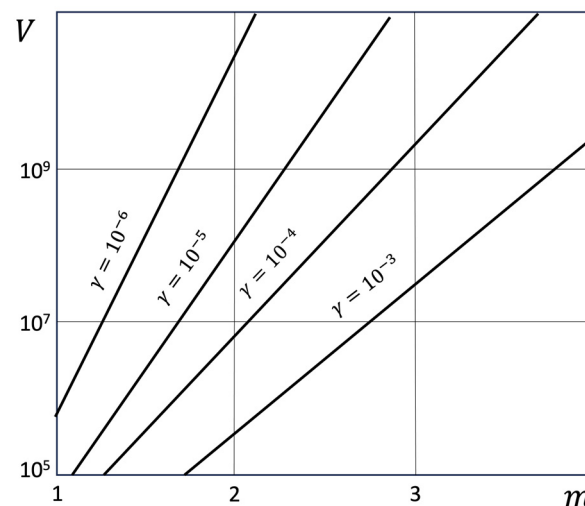


Figure 5. Factor of channel availability improvement for proposed strategy compared with traditional one.

The analysis of Figure 5 underscores the substantial benefits of implementing cross-domain redundancy in RED/BLACK communication systems. It shows that the ability to access BLACK domain resources when RED domain reserves are exhausted can dramatically improve overall system reliability, particularly in systems with inherently reliable components. This approach offers a powerful method for enhancing the resilience of critical communication infrastructure without the need for extensive additional hardware investments in the high-security RED domain.

The graph illustrates that the channel availability in the RED domain increases when the number of standby radios m in the BLACK domain increases. At the same time, the availability of channels dramatically increases with the increased reliability of the radio stations.

The implementation of the RED/BLACK concept in air traffic management communication systems introduces a robust framework for maintaining the integrity and security of classified and unclassified information. The study of the efficiency of cross-domain redundancy by leveraging BLACK domain resources for bolstering RED domain reliability reveals several key insights.

The analysis of a cross-domain redundancy strategy reveals substantive reliability improvements in the high-assurance RED domain by leveraging the BLACK domain's backup resources. The flexibility of controlled resource sharing counters the limitations of isolated RED/BLACK architectures.

The Markov model affirms the integration of supplemental BLACK radios significantly enhancing RED channel availability. The reliability factor's mathematical invariance for highly reliable systems cements the approach's applicability across varied network configurations and scales. Additionally, the selective pooling of BLACK backups for RED needs aligns with emerging standards on managing costs and complexities for mission-critical networks through dynamic redundancy. The model-based methodology demonstrates quantifiable reliability gains from such architectures.

Currently, aviation communication systems are subject to stringent requirements, including the "five nines" availability standard, which translates to a system being operational with a probability of 0.99999 [34]. This level of reliability is critical in ensuring continuous and secure communication channels, which are vital for safe and efficient air traffic management. Modern redundant radio communication channels in air traffic control systems are designed to meet or exceed this availability standard, already providing a channel availability of at least 0.99999 [35]. The approaches to ensuring reliability that are proposed in this article, particularly the cross-domain redundancy strategies, are designed to further enhance this availability.

As demonstrated in Figure 5, the implementation of the proposed reserve management strategies can lead to a significant increase in the availability of communication channels. The graph clearly shows that these strategies have the potential to increase availability by orders of magnitude, thereby moving beyond the already stringent “five nines” benchmark. The approaches presented in the study significantly enhance the reliability and availability of communication channels in aviation systems, making them even more resilient and capable of meeting the highest industry standards.

In comparing the results to prior studies, we observe that the proposed strategies for cross-domain redundancy management offer significant improvements in system reliability. For example, unlike traditional approaches that often rely on static redundancy configurations, proposed dynamic resource allocation strategies provide greater flexibility and robustness. Specifically, the use of cross-domain resource sharing, as demonstrated in the Markov chain analysis, results in a marked increase in channel availability, surpassing the reliability benchmarks reported in previous works [35]. This advancement is particularly evident in scenarios with limited redundant resources, where our strategies demonstrate superior performance in maintaining high availability under failure conditions.

At the same time, the cross-domain redundancy approach optimizes resource utilization since the BLACK radios provide additional redundancy only when needed, rather than being dedicated RED backups. The flexibility afforded by the ability to utilize radios across domains has tangible advantages over a siloed redundancy strategy. The cost savings from reduced hardware needs while maintaining high redundancy are significant.

However, the discussion must also consider potential limitations and challenges involved in implementing this cross-domain redundancy. The model does not yet account for specific RED selection logic for BLACK reserves. Moreover, the instant cross-domain switchover assumptions require validation against scenarios with encrypted session migrations. Analyzing associated switching device vulnerabilities could strengthen trust arguments.

This study contributes to the current body of knowledge by offering a theoretical model for enhancing communication reliability within the specialized context of air traffic management. However, it also provides practical considerations for the design and implementation of these systems. The proposed model and findings emphasize the critical role of dynamic redundancy and cross-domain resource utilization in strengthening the reliability of ATM communication systems, particularly those operating within the RED domain.

Future work should focus on refining the Markov model to include considerations for the strategy of selecting m radio stations from the BLACK domain and exploring the impact of non-instantaneous switching devices. Additionally, further empirical validation of the model in operational settings would be beneficial to substantiate the theoretical findings and to fine-tune the model for practical applications in air traffic control systems worldwide.

While the application of Markov chain models has provided valuable insights into the reliability of dual-priority communication systems, it is important to acknowledge the limitations of this approach, particularly in relation to state space explosion. The strategies we employed, such as state aggregation and model simplifications, are effective for managing the complexity, but there are scenarios where the number of states may still become large, making exact solutions computationally challenging. Future research could explore alternative modeling techniques, which may offer a more scalable approach to analyzing systems with extensive state spaces. Additionally, further investigation into hybrid models that combine Markov chains with other methods could provide a balanced solution to the state space explosion problem.

Future research could explore the application of alternative modeling formalisms, such as stochastic reward networks (SRNs) [36,37] and multidimensional universal generating functions (MUGFs) [38–40], which have demonstrated efficacy in characterizing modern and complex network architectures. SRNs could provide a more nuanced analysis of the reliability and performance of dual-priority communication systems, particularly in environments like 5G networks, where system states and rewards can vary significantly. MUGFs, on the other hand, could offer a scalable solution for analyzing the reliability

of multi-tenant service function chains, potentially overcoming the limitations posed by state space explosion in traditional Markov models. These approaches represent promising directions for further enhancing the robustness and applicability of reliability models in complex communication systems.

6. Conclusions

The paper presents a comprehensive investigation into improving the resilience of aviation communication systems with RED/BLACK environments through cross-domain redundancy. By developing and analyzing Markov reliability models, the paper has quantified the substantial gains achievable in the mission-critical RED domain by leveraging supplemental BLACK backups when contingencies exhaust native reserves.

The study introduces two distinct algorithms for managing cross-domain redundancy: a unified reserve pool and a separate pool approach. Both strategies demonstrate significant improvements in reliability compared to traditional isolated architectures, with the separate pools approach showing promise in scenarios with a high number of reserve elements.

There are some key findings of the study:

- Cross-domain redundancy significantly enhances overall system reliability.
- The separate pools algorithm, where the RED domain accesses BLACK domain resources only after exhausting its own, proves more advantageous as the number of reserve elements increases in both domains.
- For highly reliable systems, the reliability improvement factor remains stable across varying numbers of communication channels, indicating the model's applicability across different network scales.
- The proposed strategies offer a balanced approach to redundancy, effectively improving reliability while managing system complexity and cost.

Controlled integration, enabled through a layered reliability model and failsafe mechanisms, can significantly enhance communication resource efficiency in air traffic control systems.

The methodology and results presented constitute a compelling argument for the sharing of resources across security domains to enhance system-wide reliability. This approach not only improves operational resilience but also optimizes resource utilization, potentially leading to cost savings in system design and implementation.

Future work should focus on refining the model to include specific selection strategies for BLACK domain resources, exploring the impact of non-instantaneous switching mechanisms, and conducting empirical validation in operational settings. Additionally, investigating the application of these models to other critical infrastructure systems could further broaden the impact of this research.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Mellette, W.M.; Snoeren, A.C.; Porter, G. P-FatTree: A Multi-Channel Datacenter Network Topology. In Proceedings of the 15th ACM Workshop on Hot Topics in Networks (HotNets '16), New York, NY, USA, 9–10 November 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 78–84. [\[CrossRef\]](#)
2. Párraga Niebla, C.; Mulero Chaves, J.; De Cola, T. Design Aspects in Multi-channel Public Warning Systems. In *Wireless Public Safety Networks 2*; Câmara, D., Nikaein, N., Eds.; Elsevier: Amsterdam, The Netherlands, 2016; pp. 227–261. [\[CrossRef\]](#)
3. Gallagher, S.; Olson, M.; Blythe, D.; Heletz, J.; Hamilton, G.; Kolb, B.; Homans, A.; Zemrowski, K.; Decker, S.; Tegge, C.; et al. Communications System Architecture Development for Air Traffic Management and Aviation Weather Information Dissemination. NASA/C R—2000-210343. 2000. Available online: <https://ntrs.nasa.gov/api/citations/20010049384/downloads/20010049384.pdf> (accessed on 26 July 2024).
4. Pleter, O.T. Air Traffic Management. In *Air Navigation*; Springer Aerospace Technology; Springer: Cham, Switzerland, 2024; pp. 673–752. [\[CrossRef\]](#)

5. Awang Man, A.; Che Hussin, A.; Saktioto, O. Air Traffic Management System Business Process Analysis for the Development of Information Exchange Interoperability Framework. In Proceedings of the Eighth International Congress on Information and Communication Technology, London, UK, 20–23 February 2023; Lecture Notes in Networks and Systems. Springer: Singapore, 2023; Volume 693, pp. 919–930. [\[CrossRef\]](#)
6. Li, S.; Zang, Z.; Cheng, X. Reliability Analysis of an Air Traffic Network: From Network Structure to Transport Function. *Appl. Sci.* **2020**, *10*, 3168. [\[CrossRef\]](#)
7. Tahir, S.; Shahbaz, M.A.; Tahir, H.; Awais, M.; Khan, F.; Tahir, R.; Saeed, S.; Almuhaideb, A.M. A Novel Approach to Reduce Breaches of Aircraft Communication Data. *Electronics* **2023**, *12*, 172. [\[CrossRef\]](#)
8. Gurtov, A.; Polishchuk, T.; Wernberg, M. Controller–Pilot Data Link. *Commun. Security. Sens.* **2018**, *18*, 1636. [\[CrossRef\]](#)
9. Lee, S.-H.; Kim, Y.-K.; Han, J.-W.; Lee, D.-G. Protection Method for Data Communication between ADS-B Sensor and Next-Generation Air Traffic Control Systems. *Information* **2014**, *5*, 622–633. [\[CrossRef\]](#)
10. ABB. *Mission-Critical Communications: Let's Connect*; ABB: Zurich, Switzerland, 2019. Available online: https://library.e.abb.com/public/4413ef74a8384821b4c370e03e346317/4CAE000686_ABB_MissionCriticalControl_Brochure_A4_AirTrafficManagement_Web-r1.pdf?x-sign=cwQ+mOQ3OZWOMGPtwIV9ohba9k5hlCfqm4hhOHoNpFiAO5FH2UEgshuZGNPrUIQ (accessed on 26 July 2024).
11. Kabashkin, I. Resilient Communication Network of Air Traffic Management System. In Proceedings of the 2016 Advances in Wireless and Optical Communications (RTUWO), Riga, Latvia, 3–4 November 2016; pp. 156–160. [\[CrossRef\]](#)
12. Özmen, S.; Hamzaoui, R.; Chen, F. Survey of IP-based Air-to-Ground Data Link Communication Technologies. *J. Air Transp. Manag.* **2024**, *116*, 102579. [\[CrossRef\]](#)
13. Kabashkin, I. Dependability of Multichannel Communication System with Maintenance Operations for Air Traffic Management. In *Engineering in Dependability of Computer Systems and Networks, Proceedings of the Fourteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, Brunów, Poland, 1–5 July 2019*; Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., Eds.; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2020; Volume 987, pp. 256–263. [\[CrossRef\]](#)
14. SITTI. Advanced Military Communication Features. 2021. Available online: <https://www.sitti.it/wp-content/uploads/2021/04/MKT.0006.EN-rev.3.0-FunzioniMilitari.pdf> (accessed on 26 July 2024).
15. ISODE. Red/Black Web-Based HF Radio System Monitoring. Available online: <https://www.isode.com/products/red-black.html> (accessed on 26 July 2024).
16. Frequentis. *Telebrief—Secure Mission-Critical Briefing System*; Frequentis: Vienna, Austria, 2023. Available online: https://www.frequentis.com/sites/default/files/support/2020-01/54_DEF_Telebrief_1219.pdf (accessed on 26 July 2024).
17. L3Harris. THE MOMENTUM: Secure Communications for Mission Critical Audio. Available online: <https://www.l3harris.com/all-capabilities/momentum-ics> (accessed on 26 July 2024).
18. C4i. VOICE C2 Red/Black. Available online: <https://www.c4i.com/en/products> (accessed on 26 July 2024).
19. Rohde & Schwarz. *R&S®M4ACS Air Domain Communications System: Trusted Communications for Safe Air Traffic Control and Air Defense*; Product Brochure; Rohde & Schwarz: Munich, Germany, 2023. Available online: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/pdm/cl_brochures_and_datasheets/product_brochure/3684_1014_12/M4ACS_bro_en_3684-1014-12_v0100.pdf (accessed on 26 July 2024).
20. SAAB. AviCom: Radio & Audio Management System. Available online: https://www.saab.com/globalassets/products/ips/avicom---radio--audio-management-system/avicom_general-brochure.pdf (accessed on 26 July 2024).
21. Orion Systems Inc. Secure Mobile Communications with KYoIP. Available online: <https://www.orionsystemsinc.net/secure-mobile-communications/> (accessed on 26 July 2024).
22. Zheng, R.; Li, X.; Chen, Y. An Overview of Cognitive Radio Technology and Its Applications in Civil Aviation. *Sensors* **2023**, *23*, 6125. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Leuchter, J.; Bloudicek, R.; Boril, J.; Bajer, J.; Blasch, E. Influence of Aircraft Power Electronics Processing on Backup VHF Radio Systems. *Electronics* **2021**, *10*, 777. [\[CrossRef\]](#)
24. Sanchez-Aguero, V.; Valera, F.; Vidal, I.; Nogales, B. Communication Manager for Hyper-Connected RPAS Environments. *Drones* **2023**, *7*, 137. [\[CrossRef\]](#)
25. Cheng, Y.; Zhou, Z.; Li, R.; Li, J.; Wang, J.; Pei, X. Reliability Prediction and Safety Evaluation of ATC Automation System. In Proceedings of the 2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT), Weihai, China, 14–16 October 2020; pp. 969–972. [\[CrossRef\]](#)
26. Zahra, K. Misleading Communication vs. Effective Aviation Management. *Intell. Inf. Manag.* **2011**, *3*, 240–243. [\[CrossRef\]](#)
27. Zhang, L. Preliminary Exploration of the Reliability of Civil Aviation ATC Communication Network. *J. Phys. Conf. Ser.* **2020**, *1533*, 022043. [\[CrossRef\]](#)
28. EUROCONTROL Experimental Centre. *Implications of End-to-End Communication for Air Traffic Control*; EEC Technical/Scientific Report No. 2009-012; EUROCONTROL: Brussels, Belgium, 2009. Available online: https://www.eurocontrol.int/sites/default/files/library/023_End_to_end_communications_in_ATC.pdf (accessed on 26 July 2024).

29. Kleinert, M.; Helmke, H.; Shetty, S.; Ohneiser, O.; Her, H.; Prasad, A.; Motlicek, P.; Harfmann, J. Automated Interpretation of Air Traffic Control Communication: The Journey from Spoken Words to a Deeper Understanding of the Meaning. In Proceedings of the 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 3–7 October 2021; pp. 1–9. [\[CrossRef\]](#)
30. Levin, E.; Zaynal, S. Voice Communication System for Air Traffic Control—Development and Evaluation of a Prototype. Master's Thesis, University of Gothenburg, Göteborg, Sweden, 2011. Available online: <https://publications.lib.chalmers.se/records/fulltext/155125.pdf> (accessed on 19 November 2023).
31. Rohde & Schwarz. *R&S®GV4000 Multi-Link Controller: High-Availability ATC Radio System*; Product Brochure; Rohde & Schwarz: Munich, Germany, 2016. Available online: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/service_support_30/GV4000_dat_en_5214-2240-32_v0300_96dpi.pdf (accessed on 26 July 2024).
32. Rubino, G.; Sericola, B. *Markov Chains and Dependability Theory*; Cambridge University Press: Cambridge, UK, 2014.
33. Kabashkin, I. Dynamic Redundancy in Communication Network of Air Traffic Management System. In *Advances in Dependability Engineering of Complex Systems, Proceedings of the Twelfth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Brunów, Poland, 2–6 July 2017*; Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., Eds.; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2018; Volume 582, pp. 178–185. [\[CrossRef\]](#)
34. Communications Operating Concept and Requirements for the Future Radio System. EUROCONTROL/FAA Future Communications Study Operational Concepts and Requirements Team, Version 1.0. 2006. Available online: <https://www.icao.int/safety/acp/Inactive%20working%20groups%20library/ACP-WG-C-10/WGC10-WP04-COCR%20V1.0.pdf> (accessed on 24 August 2024).
35. *iSecCOM: Mission-Critical Secure Communications*; Frequentis AG: Vienna, Austria, 2024. Available online: https://www.frequentis.com/sites/default/files/support/2024-05/iSecCOM_product-brief_DEF_Frequentis.pdf (accessed on 24 August 2024).
36. Cicirelli, F.; Nigro, L. Analyzing stochastic reward nets by model checking and parallel simulation. *Simul. Model. Pract. Theory* **2022**, *116*, 102467. [\[CrossRef\]](#)
37. Angius, A.; Horváth, A. Analysis of stochastic reaction networks with Markov reward models. In Proceedings of the 9th International Conference on Computational Methods in Systems Biology, CMSB '11, Paris, France, 21–23 September 2011; ACM: New York, NY, USA, 2011; pp. 45–54. [\[CrossRef\]](#)
38. Arakawa, K.; Oki, E. Availability-aware virtual network function placement based on multidimensional universal generating functions. *Int. J. Netw. Manag.* **2024**, *34*, e2252. [\[CrossRef\]](#)
39. Jafary, B.; Fiondella, L. A universal generating function-based multi-state system performance model subject to correlated failures. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 16–27. [\[CrossRef\]](#)
40. Levitin, G. A Universal Generating Function in the Analysis of Multi-state Systems. In *Handbook of Performability Engineering*; Misra, K.B., Ed.; Springer: London, UK, 2008; pp. 447–464. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.