Towards the use of public networks for safety-related aeronautical communications

Cyril Louis-Stanislas, Stephane Tamalet, Jose Radzik, Emmanuel Lochin

Towards the use of public networks for safety-related aeronautical communications

Cyril LOUIS-STANISLAS
PhD student – IYACC
AIRBUS Operations S.A.S.
Toulouse, France
cyril.louis-stanislas@airbus.com

Stephane TAMALET
Communication & Sensing Systems – IYACC
AIRBUS Operations S.A.S
Toulouse, France
stephane.tamalet@airbus.com

Jose RADZIK
ISAE-SUPAERO
Toulouse University
Toulouse, France
jose.radzik@isae-supaero.fr

Emmanuel LOCHIN
ENAC
Toulouse, France
emmanuel.lochin@enac.fr

***Abstract*—Aircrafts are increasingly equipped with in-flight connectivity systems, giving access to broadband communications for passengers. This paper studies whether it may be possible to use these public air-ground networks to also support aircraft safety-related aeronautical communications in the future. The benefits and other justifications are also examined, including the challenges and potential 'showstoppers'. It provides a risk and a SWOT analysis and introduces potentially suitable technical mechanisms.**

***Index Terms*—Aeronautical communications, Data link, Commercial networks, Hybrid architecture**

I. Introduction

Commercial aeronautical networks are receiving more and more attention from various aeronautical stakeholders (e.g., International Civil Aviation, airlines, avionics, etc.). Moreover, with the next generation of public access networks (i.e., 5G cellular networks, satellite internet proposed by Starlink, Kuiper or Telesat), commercial aeronautical networks will be faster, cheaper, and more reliable. In fact, these networks are now excellent candidates to support safety-critical aeronautical communications that still use relatively aging and expensive technology.

The number of commercial aircraft offering in-flight connectivity (IFC) services to their passengers (for web browsing, social networks, audio and video streaming) is growing rapidly. Furthermore, the quality of service provided to the passengers, and the emergence and adoption of improved connectivity solutions, lead to an increasingly competitive market. To meet this growing demand and provide the best possible passenger experience, airlines are now equipping their aircraft with broadband communications systems, such as Ku/Ka-band satellite communication systems. These IFC systems are increasingly capable of offering more network capacity, less delay, and improved reliability.

On the other hand, safety-related aeronautical communication systems (in red, see Figure 1), for instance, used for Air Traffic Control (ATC) communication, operate with legacy systems, such as, Aviation VHF, HF, and authorized L-band satellite systems, which are based on relatively aging technologies. As safety-related aeronautical communication use-cases become increasingly stringent in terms of performance requirements, this paper proposes to investigate how public commercial aeronautical networks could support and be beneficial in carrying safety-critical aeronautical communications.

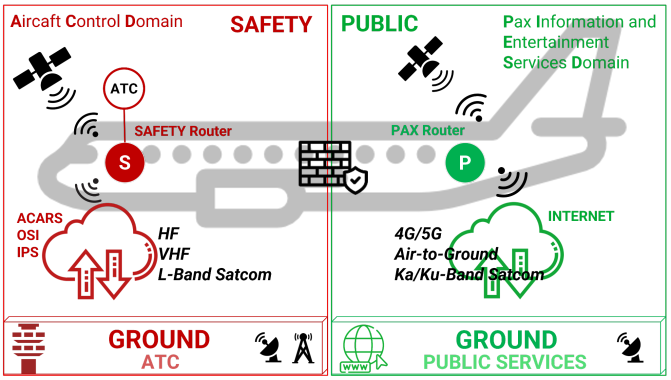

Fig. 1. Aircraft communication architecture overview

This paper follows the same objectives as the SESAR project 14/Solution 61-HyperConnected ATM, which studies whether or not public open commercial networks could be used to support data safety-related communications.

This paper is organized as follows: Section II identifies justifications and benefits for this concept; Section III comprises a discussion of potential 'showstoppers'; Section IV includes a risks analysis; Section V summarizes all previous sections with a Strength, Weakness, Opportunities, and Threat (SWOT) analysis; Section VI proposes high-level technical principles that could tackle the challenges and offers a solution for a targeted objective; Section VII outlines future work; and finally, Section VIII concludes.

II. Justifications and Benefits

A. Spectrum shortage

Safety-related communications are operated within dedicated and protected spectrum bands.

The spectrum currently allocated to safety-related communication services is becoming increasingly congested [1]. VHF data traffic is at risk of suffering performance degradation in the not-too-distant future in areas with a high density of air traffic. It may be difficult to operate the next safety-related communication services generation on such a limited spectrum, therefore, the frequency band currently available for aeronautical services should be expanded. However, it is not easy to find new, available spectrum because of the intense competition between numerous stakeholders for this rare resource. Furthermore, the cost and time needed to deploy a new system in a non-used spectrum (such as band C) would be prohibitively expensive.

The use of public networks to support data safety-related communications could be a solution to this spectrum shortage issue.

B. Supporting ATM[1] system future needs

It is without doubt that over time, and with the emergence of new use cases (such as 4D Trajectory Based Operation) and new forms of air traffic (including Urban Air mobility, RPAS, High Altitude Platforms etc.), the needs of safety-related communications will dramatically increase [2]. Thus, to operate optimally in this new and rapidly-evolving environment, aeronautical communications will require more capacity. Unfortunately, for reasons of costs, scaling, slow standardization, technological limitations, or international interoperability, the transition to a new safety-related communication system may not be rapid enough [3]. This leads us to a situation in which the current system faces significant difficulties in supporting the needs of anticipated safety-related services in the future.

Thus, by combining both current legacy safety-related communications systems, and current open public systems in hybrid architecture, it may be possible to increase overall capacity, and thus support ATM system future needs.

C. Cost effectiveness

The use of public networks for supporting safety-related communications could be cost effective because:

- public ground/air-ground infrastructure has already been developed, deployed, and validated. Aircraft are already equipped with avionics equipment designed to support non-safety critical cockpit communications, as well as cabin/passenger communications. We can therefore consider that limited investments will be necessary in this area in the short term;
- public communication (usage/OPEX) costs are generally three orders of magnitude lower than those of air-ground networks that are specifically designed and dedicated to support safety communications [4];
- interoperable and implemented public solutions (such as WIFI Cellular) can allow the same equipment to be reused across regions. Moreover, these public systems may benefit from reduced equipment costs thanks to the competition within this sector, plus the massive amortization of non-recurring costs, and the optimization of recurring production costs;
- relying on complementary public communications solutions could contribute to tempering the congestion issues on legacy safety communication infrastructure, and hence protect the investments already made for the legacy fleet. Open architecture may also offer the long-term upgradability and scalability of ATM service provision and the agility/affordability required to enhance services.

D. Global interoperability and coverage

The public networks, using technology based on or derived from open standards (e.g., 3GPP), have high synergies with mainstream mobile networks. This guarantees the air-ground interoperability of equipment between different suppliers, as well as an interoperable terminal-infrastructure interface on the ground. The solution can also allow global or regional interoperability as it uses global (Ku/Ka sat, Airport 4G/5G) or regional (A2G) infrastructure operated on a licensed spectrum.

E. Other considerations

Beyond commercial airlines, other user groups (such as helicopters, general aviation, RPAS, Urban Air Mobility, and business aviation) could benefit from this solution. Integrating a public communication solution could be a practical way to augment the basic legacy communication capabilities of these currently constrained platforms.

III. POTENTIAL SHOWSTOPPERS

In this section, we explore the main challenges to the use of public networks in support of safety-related aeronautical communications.

A. Spectrum regulation

Current spectrum regulation relies on two main entities: the International Telecommunication Union (ITU) and the International Civil Aviation Organization (ICAO).

While ITU has to consider frequency sharing (to increase spectrum efficiency) [5], ICAO regulations mandate that safety communications must be supported by technologies operated in a protected spectrum and reserved for safety services [1] [6]. This is a potential showstopper in terms of using commercial networks to support safety-related traffic.

However, the following considerations could potentially overcome this challenge:

[1] Air Traffic Management

- modify the ICAO policy and integrate the exceptions that take into account the use of public networks under certain conditions (mechanisms, notably);
- carefully confirm that the ultimate goal of the ICAO policy is not intended to prohibit the use of public networks, but rather to ensure that their systems perform at the right level of safety. As long as this condition is respected, ICAO regulation is no longer a showstopper;
- mitigate safety issues (such as interference, capacity, radio equipment failure probability, etc.) with appropriate mechanisms, in such a way that safety constraints on using public networks could arguably be removed if failures have no safety effect.

B. Certification issues

Certification is one of the processes used to manage and ensure common and harmonized safety levels in aviation. It is very common in civil aviation that compliance to some requirements is demonstrated through certificates issued by a competent authority for the system, the crew or a particular component after undergoing a process known, understood, and recognized by all the actors. In certain cases, regulations may allow delegation of the ability to sign certificates to recognized organizations.

It will then be necessary to ensure that the considered solution does not violate or fail to meet the certification requirements, which would require the following:

- work towards a solution that incorporates mechanisms to totally mitigate the impacts of failures on commercial links, in such a way that it can be demonstrated that the use of commercial links is completely free of safety impacts;
- complete the ICAO standardization of the solution mechanisms, so that it becomes a standard technology formally recognized as suitable to support safety critical communications. It would then become possible to update the certification framework to integrate the solution as a possible Accepted Means of Compliance (AMC) [7].

C. Performance requirements

Performance requirements are prescribed by a State for communication or surveillance capability under the form of RCP[2]/RSP[3] specifications. They define four performance parameters: transaction time, continuity, integrity, and availability [8] [9].

The transaction time (TT) sets an upper bound time-limit, not to be exceeded when transferring safety data. TT can be for one-way or two-way data exchanges, however, when using commercial links and public Internet, performance is not guaranteed. The services are generally provided along a 'best effort' approach, and the quality of service may vary unpredictably. A solution is therefore needed to ensure that end-to-end TT will be consistently achieved. Section VI-A describes possible mechanisms to address this issue.

Regarding *Integrity*, RCP/RSP specifications are based on a safety assessment of the effects of undetected data corruption or misdirection in the context of intended use. However, the integrity hazards are mitigated end-to-end (at the application level) by strong integrity check mechanisms, which ensure with a very high level of probability that any data message received with random errors applied will have a wrong CRC and will consequently be detected. The probability of random failures going undetected (such as, corruptions, misdirection, etc.) within commercial links, (such as the public Internet) is then extremely remote.

Availability is the probability that an operational communication transaction can be initiated when needed. *Continuity* is the probability that an operational communication transaction can be completed within the transaction time. Given that the very concept of the subject is to use public links besides safety links, this, by definition, increases the path diversity of safety data, and hence offers an opportunity to improve availability and continuity. Nevertheless, some mechanisms (see Section VI-A) are needed to ensure that data flows always use an available path and are redirected in a timely manner when the preferred path becomes unavailable.

D. Safety requirements

Today, losing safety data link communication is classified as a MINOR event. This MINOR classification implies the need to use a radio link whose elements are developed with a DAL-D quality level [10] [11]. However, public networks use components that are not developed with effective enough processes to guarantee the DAL-D quality level. They are therefore generally considered as DAL-E links. Consequently, exclusively using open networks to support safety-related communication does not meet safety requirements.

To address this issue, a possible solution is to consider public links as additional paths (besides safety links), which could support safety-related traffic. Thus, with appropriate mechanisms, using commercial networks within a hybrid architecture should no longer have safety impacts, as long as all the safety-related traffic can be time-efficiently recovered on the safety network. However, one showstopper remains: the undetected loss of public links.

The undetected loss of a commercial link, which may become a routing black hole and lead to the loss of end-to-end communications, is the main overall problem to be addressed. As this failure case can have a safety impact, mitigation mechanisms are imperative, which must be

[2] Required Communication Performance

[3] Required Surveillance Performance

developed at an assurance level commensurate with the severity of the associated event, and be able to contain the occurrence rate of the event within the safety objective limit.

IV. Risk analysis

This section analyses potential risks linked to the use of public networks for safety-related communications:

A. Risk of losing the spectrum reserved for aviation

Over the years, ICAO has established a worldwide policy for frequency allocation in order to be protected against interference and to allow worldwide communication interoperability between all participants.

Lately, with the exponential growth of various wireless communication markets, reserved aviation spectrum is increasingly coveted. Until now, aviation stakeholders have managed to preserve their closely-guarded safety spectrum. However, because of the lack of available spectrum, aeronautical frequency bands have increasingly come under scrutiny for potential sharing with non-aeronautical services. The growing use of frequency bands adjacent to those used by aeronautical systems providing safety critical Communications, Navigation, and Surveillance functions is already bringing the risk of potential harmful interference to aeronautical systems.

The use of commercial networks for safety-related data in aeronautical communications could create a weakness in aviation spectrum defense. This could be exploited by other sectors as an argument to support their claim to get shared access to the aeronautical spectrum.

Indeed, it is considered that this risk already exists. Some examples where the margins of the aviation spectrum have been allocated to non-aviation users are noted, necessitating specific actions and efforts of the aviation community to mitigate the risks of interference. This will happen increasingly more often in the future. Therefore, instead of being considered as a potential risk, this study may be considered a proactive way to find an alternative to an inevitable event.

B. Cybersecurity risks

The use of public links introduces cybersecurity threats.

A malicious attack can attempt to target aeronautical communications (e.g., by overloading the networks or by injecting erroneous information). Such an attack could also potentially use this attack path to reach other parts of the aircraft's or ground's aeronautical network infrastructure.

This risk can be analyzed and hopefully mitigated with appropriate security mechanisms, yet to be determined.

C. Risks of interruption to the commercial service

Commercial network service providers work on a 'best effort' model, within which there is no strong guarantee of long-term service continuity or availability. This means that for various reasons (financial, geopolitical, technological obsolescence, business strategy, etc.) a public network service provider can decide to stop providing their services.

This risk will be mitigated, however, by the same mechanisms that will be used to mitigate transient failures on the public links.

D. Risks of non-dissimilarity and common point of failure

One of the advantages of using commercial networks for safety related data is to increase the path diversity of the traffic, and hence to increase continuity and availability. Nevertheless, in general, there is no guarantee that commercial networks are using technologies that are fully dissimilar to, or have no common failure mode with the alternate paths. While the objective has been to provide diversity and dissimilarity for the routing of safety traffic, the risk is to expose the data exchanges to a common point of failure.

This point is important, but is not considered to be a showstopper. This is because the use of public links is proposed to be used only as complementary segments to a fallback baseline safety-qualified communication infrastructure. Then, in the worst case, where the commercial segments would be hypothetically 100% similar and common to the baseline fallback segment, with 100% common failure modes, the availability and continuity of the end-to-end service would at least stay equivalent to that of the baseline safety-qualified communication infrastructure. From this hypothetical worst case similarity bottom line, the added public link can also introduce dissimilar components, which will then *de facto* enhance the availability and continuity of the overall system.

V. SWOT Analysis

Having highlighted and addressed potential solutions to all the transversal problems, it appears that there are no strong contraindications in using public commercial aeronautical networks for safety-critical aeronautical communications. Strengths, weaknesses, opportunities, and threats of this concept, are summarized in a SWOT analysis below:

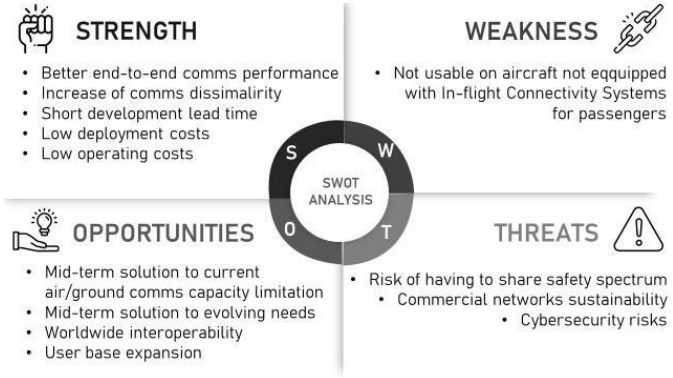

Fig. 2. SWOT Analysis

VI. TECHNICAL SOLUTION UNDER STUDY

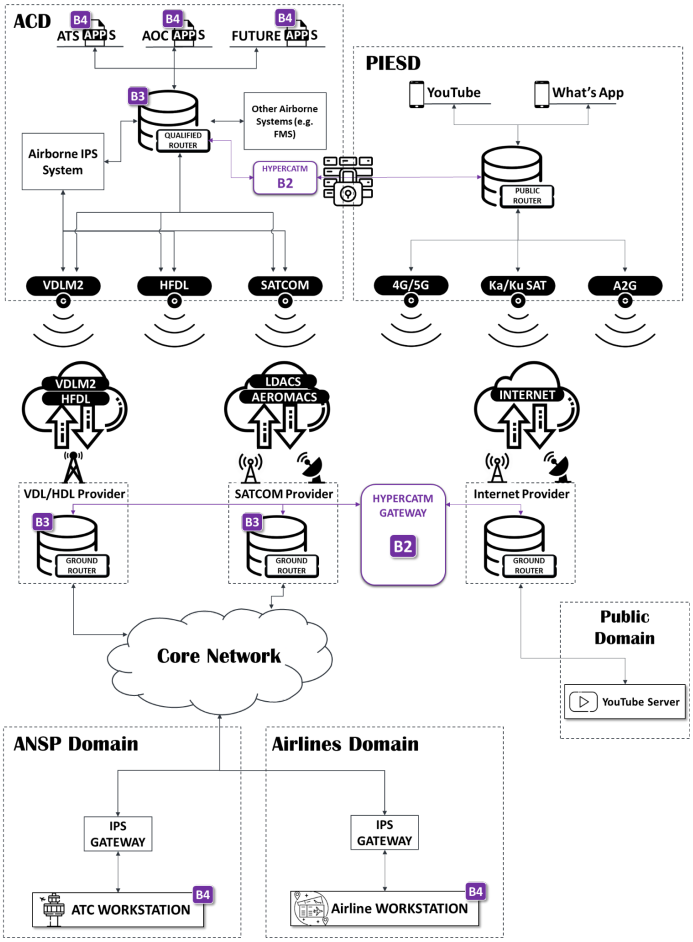

Fig. 3. Hybrid architecture of the concept

For safety considerations (see Section III-D), Figure 3 presents a hybrid architecture where safety networks and public networks could exchange data with each other. The purple boxes indicate strategic locations where it would be necessary to implement mechanisms, so that the concept meets all identified requirements. Some of them are briefly described below.

A. Mechanisms

In its most basic use, some mechanisms are **required** for this concept to be feasible:

1) Fall-back: In this concept, the fall-back mechanism aims to mitigate safety issues. For the public networks to be considered as a complementary path with no safety impact, this mechanism must perform two main actions:

- timely detection when an attempt to transfer a message over a public link may have gone wrong, and;
- timely retransmission in due time to remain compliant with the end-to-end RCP time and continuity requirements.[3]

2) Acknowledgment monitoring: this mechanism is the key element for the timely detection of the loss of connectivity and is therefore crucial for the fall-back mechanism. It keeps track of all packets transmitted through public networks and monitors whether or not they are time-effectively acknowledged. If not, an alert is raised to inform other mechanisms responsible for decision-making to either retransmit on public links or on safety ones (such as the fall-back mechanism). The time after which the alert is raised must be configured according to RCP requirements.

3) Messages inspection/Firewalling: This mechanism aims to mitigate security and cyber-security issues. As a classical firewall, it monitors incoming and outgoing network traffic and decides whether or not to allow or block specific traffic based on a defined set of security rules. There are different types of firewalls, such as a proxy firewall, a stateful inspection firewall, a unified threat management firewall, a virtual firewall, and so on, and all could potentially be used to fulfill this requirement. The final choice is outside the scope of this paper.

4) Virtual Private Network: VPN mechanisms (such as the ATN/IPS concept), should be considered to create a secure tunnel between two trusted endpoints over a public network, for security and cyber-security considerations. There are already several VPN protocols that focus either on data throughput speed or on masking and encrypting packets. The trusted endpoints on the ground should most likely be

[3] When sufficient time is available, the fall-back mechanism could possibly attempt to make retransmission(s) on the commercial link(s) first

located at the edge of the safety communication domain, so that the message inspection mechanism[4] is not bypassed.

Nevertheless for a more evolved concept, which could support future uses cases, some other **recommended** mechanisms could be implemented :

5) Link selection and multilink: Current legacy ACARS and ATN/OSI routers already support the capability to manage alternative paths between ground and airborne end-systems, that go through different air-ground links (e.g., HFDL, VDL Mode 2 and Satcom). Following the current strategy, first they filter out the unavailable path at the present moment, based on a link status availability. Then they select, among available paths, the highest priority one, according to a predefined routing policy algorithm. Eventual retransmissions are handled by a transport layer protocol.

However in a link selection/multilink scenario where public links are involved, this process can not be applied because:

- there is a low level of assurance regarding the capability for commercial links to meet RCP requirements;
- as public links are unpredictable, the routing policy should be done dynamically;
- retransmission should be managed with the fall-back mechanism in order to avoid looping on an unavailable link and end up in a total loss of communication scenario, while other links are available.

The alternative ”delayed flip-flop multi transmission” strategy would most likely fit in a link selection/multilink scenario where public links are involved. The process is as follows:

- (FLIP) transmits a first copy of the original ATC message over a first air-ground link/path (e.g., a public link), and;
- (DELAYED FLOP) later transmits, only if needed (i.e., if not already acknowledged by the ground), a second copy of the original message along an alternate air-ground link/path (e.g., a safety link).

Besides having a good synergy with the link status monitoring mechanism alternative strategy (see Section VI-A2), a delayed flop transmission time greater than a nominal acknowledgement time (note that the ack time on public should be very short) could, in most cases, prevent useless retransmission, and therefore save some costs while meeting safety and performance requirements.

Some other alternative strategies (such as, the PerformanceBased Multilink Approach [12], the end-to-end mobility management [13], or the 5G 3GPP multi link mechanism) could also fit in a selection/multilink scenario where public links are involved and are more fully described in the SESAR Hyper Connected ATM concept definition.

6) Link status monitoring: The goal of the link status monitoring mechanism is to provide an appropriate level of assurance regarding the status[5] of the air-ground connectivity through the public link(s). This status is the key element for the timely detection of loss of connectivity and is therefore crucial for the fall-back mechanism (see SectionVI-A1). A common way to achieve link status monitoring is through periodic probing. However, if this is completed frequently, it can be very bandwidth consuming (and increase communication costs).

7) Link performance monitoring: Although it uses the same probing technique as link status monitoring, link performance monitoring aims to gather metrics’ performance. The objective is to compare the measured performance to a calculated required time to transmit data on a safety link, based on the data criticality. This comparison provides a guide as to the ability of the commercial link to transmit the data fast enough, to fall back on a safety link in case of failure, so that performance requirements are met in any case.

B. The overall combination

Thus, it appears that the technical solution relies on the combination and collaboration of several mechanisms, which must ‘complete’ each other to ensure that the end-to-end communication safety and performance requirements are met. To have a better overview and understanding on how this concept could manage all these mechanisms, it is possible to group them into three separate classes:

- security mechanisms;
- virtual overlay radio mechanisms;
- risk- and performance-based multilink principle mechanisms.

[4] Mandatory

[5] Either available or not

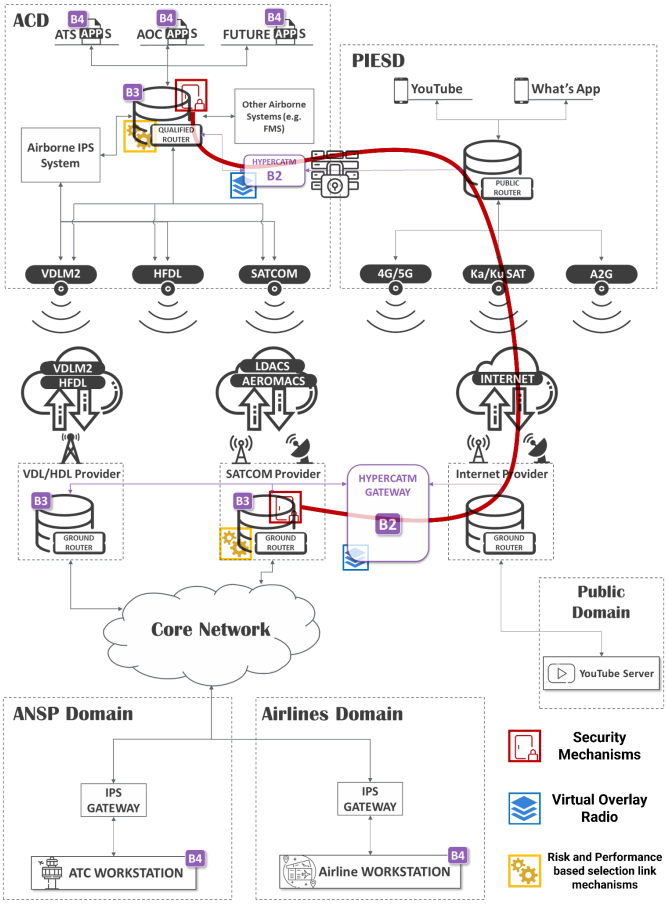

Fig. 4. Overall combination

1) Security mechanisms: These must provide a high level of confidence that any attacks coming from public links can be detected and countered. To do so, these security functions are intended to be hosted within trusted domains of the aircraft and the ground counterpart, within the infrastructure of a trusted organization involved in aeronautical safety communications (note the red area on Figure 4). In this class, mechanisms (such as VPN tunnel, firewalling functions, deep packet inspection functions, or additional E2E security functions) should be expected.

2) Virtual Overlay Radio mechanisms: These must gather and provide useful information (link status/performance, transaction history, etc.) to the system. These mechanisms must be defined independently from the underlying commercial networks in order to enable interoperability between the aircraft and the ground. Finally, they should be developed at the appropriate DAL.

3) Risk- and Performance-based selection link principle mechanisms: These mechanisms are responsible for making the decision to transmit (or not) on public commercial links, based on all information and variables gathered by Virtual Overlay Radio mechanisms.

VII. FUTURE WORK

There will be two points of focus in future work: the mechanisms themselves; and their overall combination.

Regarding the mechanisms themselves, a deeper study must be conducted either to validate an existing mechanism through its specifications and how it fits in the concept, or to increase existing mechanisms in order to perfectly fit the concept's needs. Considering this second point, a future work could be to emulate safety applications over public links in order to draw an analytical model that is able to predict (in most cases) when public links exceed performance requirements. With an analytical mechanism, the provided information can lead to a carefully considered and seamless switch/multilink decision between the safety domain and the public links.

Regarding the overall combination, future work would be to describe in detail how each mechanism would connect with each other and reproduce all the elements in emulation, in order to finally evaluate the concept in its integrity.

VIII. Conclusion

After the analysis of the transversal considerations of the subject, it appears that a technological solution is not only conceivable, but would make it possible to address a satisfactory response to the identified constraints. The first draft here is the initial key response to the performance and safety requirements. A more detailed study, including safety requirements and certifications, will be completed in a future paper.

References

[1] "Icao spectrum strategy, policy, statements and related information," in *Handbook on Radio Frequency Spectrum Requirements for Civil Aviation*, vol. Doc 9718, 2018.

[2] M. Prandini and J. Hu, "A probabilistic approach to air traffic complexity evaluation," in *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, 2010.

[3] T. Grobotek and V. De Vroey, "Integrated air traffic management," in *European Partnership under Horizon Europe*, 2020.

[4] "Communications costs on safety and non-safety networks," in *AIRBUS Intern Confidential Documents*, 2010.

[5] P. Curnow-Ford, J. Deaton, H. Del Monte, B. Goermmer, and J. Hane, in *The Spectrum Handbook 2018*, 2018.

[6] "Articles," in *Radio Regulations*, 2016.

[7] E. union Aviation Safety Agency, in *Acceptable Means of Compliance (AMC) and Alternative Means of Compliance (AltMoC)*.

[8] "Performance-based communication and surveillance (pbcs) manual," vol. Doc 9869, 2017.

[9] D. G. Depooter and O. Lucke, "Required communication technicalˆ performance, the application layer qos metric for aeronautical data communications," 2015.

[10] Eurocae, "Ed78a," in *Guidelines for Approval of the Provision and use of Air Traffic services Supported by data communications*, 2000.

[11] ——, "Eurocae ed-79a / sae arp 4754a," in *Guidelines for Development of Civil Aircraft and Systems*, 2010.

[12] D. Zeng, M. Niraula, and M. Niraula, "Wp03 - performance based multilink approach for ips," in *ICAO CP/WG-$I_2$6.*

[13] T. Whyman, "Wpxx – end-to-end multilink mobility management," in *ICAO CP/WG-$I_3$0.*