XXI SITRAER
2024 | Air Transportation Symposium

CONDUCTING A PRELIMINARY STPA ANALYSIS OF UNMANNED AIRCRAFT SYSTEM TRAFFIC MANAGEMENT (UTM): A CASE STUDY ON PACKAGE DELIVERY IN URBAN ENVIRONMENTS

Mauricio Antoniazzi[1]*, Rafael Albarello Hickman[2], Rafael Cenato[2], André Elias Melo[2], Celso Massaki Hirata[1], Rubens José Maleiner[1]
1 Instituto Tecnológico de Aeronáutica (ITA)
2 Instituto de Controle do Espaço Aéreo (ICEA)

*** Corresponding author e-mail address**: mauricio500@gmail.com

PAPER ID: SIT881951

ABSTRACT

With the rise in unmanned aircraft, or drones, and their increasingly advanced capabilities, new services such as package delivery in urban areas are feasible. Unmanned Aircraft System Traffic Management (UTM) supports drone delivery services by managing drone traffic. However, the management of drone traffic requires a complex safety-critical analysis. This paper applies the System-Theoretic Process Analysis (STPA) method to help in the safety analysis of a UTM system. The safety analysis allowed identifying potential hazards, unsafe control actions, possible causes, and safety recommendations to ensure the safe operation of the proposed system. The study was conducted with the help of an STPA tool named AppSTPA. The analysis is intended to subsidize the design of the BR-UTM by identifying safety-critical recommendations to the key stakeholders.

Keywords: Unmanned Aircraft (UA), Drone, System-Theoretic Process Analysis (STPA), Unmanned Aircraft System Traffic Management (UTM).

1. INTRODUCTION

In recent years, unmanned aviation has experienced significant advancements, such as introducing new and more capable unmanned aerial vehicles (UAVs), colloquially called drones. The cost-efficient nature of drones has enabled the provision of various services and even opened up new possibilities. For example, they can now be used for agricultural spraying of fertilizers and defensives at a fraction of the cost of manned aircraft. Furthermore, drones can inspect structures in challenging locations, gather images and data, and conduct property surveillance, among other services (Silva *et al.*, 2023). According to the specialized consultancy firm Drone Industry Insights (2023), the global drone market in 2023 generated almost US$ 33.7 billion in revenues, and its size is forecasted to reach US$ 54.6 billion by 2030, with an estimated compound annual growth rate of 7.1%.

Besides the already mentioned drone applications occurring in many places, there has been considerable buzz within the industry regarding the viability of drone utilization for deliveries in densely populated areas. Though delivering a pizza via drone in a bustling city may appear straightforward, it presents complex challenges that necessitate meticulous evaluations of operational factors. Among these, the safety of the drones during operation, particularly in the airspace they navigate, is a critical concern.

Drone operations are supported by the Unmanned Aircraft System Traffic Management (UTM) system. The UTM system must be able to monitor and control drones in the airspace that might be used by manned aviation. The integration of UTM systems and Air Traffic Management (ATM) systems is needed to provide safe and efficient operations for both drones and manned aircraft (ICAO, 2023).

Nowadays, drone operators reserve volumes of airspace during a limited period to access the UTM airspace beforehand. This scheme is pessimistic since the reservation periods are long and conservative. It avoids a more dynamic use of airspace. Due to the increasing number of UTM airspace requests, a more flexible scheme is required. It must cope with the growing number of requests and be safe-critical.

This work aims to present a case study of a package delivery from a shopping center to a residential condominium in an urban area using System-Theoretic Process Analysis (STPA). Using the STPA technique, a preliminary assessment of hazards, unsafe control actions, possible causes, and safety recommendations will be performed to evaluate the safety of the operation under a set of assumptions.

2. LITERATURE REVIEW

2.1 The System-Theoretic Process Analysis (STPA)

Critical safety systems are becoming increasingly more complex. These systems use software, highly powered processors, and different types of networks, operate with physical and cybernetic components, have hierarchical controls, and often must follow certification bodies' directives (Carniel *et al.*, 2023).

The STPA is a technique utilized for hazard analysis (Leveson and Thomas, 2018). Its main objective is identifying safety recommendations and constraints by considering how unsafe interactions among system components can lead to accidents. STPA draws upon the System-Theoretic Accident Model and Processes (STAMP), an accident causality model based on systems theory (Leveson and Thomas, 2018). This model surpasses the traditional causality chain that includes only directly related failure events or component failures. STPA considers more intricate processes, hazardous interactions among system components, and all potential causal factors of losses, including software and human causal factors. Plioutsias *et al.* (2018) complement that STPA is a top-down

system engineering approach to system safety that can be used early in system development to generate high-level safety requirements and constraints.

It is claimed that STPA identifies more loss scenarios and recommendations when compared to other hazard analysis techniques, such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA). However, it is a lengthy and complex process analysis (Carniel *et al.*, 2023).

The process is structured into four steps, described below (Leveson and Thomas, 2018):

- Step 1 – Define the Purpose of the Analysis. Identify system goals and boundaries, assumptions, losses, hazards, and system-level safety constraints.
- Step 2 – Model the Control Structure. Identify interactions and functional relations among the system components.
- Step 3 – Identify Unsafe Control Actions (UCA). Investigate potential UCAs and associated system constraints.
- Step 4 – Identify Loss Scenarios. Identify potential causes of the UCAs to discover loss scenarios and associated causal factors to generate safety recommendations.

A key aspect of using STPA is obtaining an adequate control structure model. The control structure model should be sufficiently complete to capture all the hazards so that the resulting analysis does not miss any loss scenario. Still, it cannot have too many details, as it would be too complex to analyze with an unmanageable number of contexts. The STPA is an interactive process that should involve several stakeholders, including experts on the system under analysis and safety specialists (Carniel *et al.*, 2023).

AppSTPA, an ontology-based tool, assists in conducting the case study. In AppSTPA, the proposed ontology helps in knowledge representation and supports reasoning and inference. Knowledge representation helps the tool´s user build the control structure more consistently, while logic and inference help to identify more comprehensive suggestions of loss scenarios and causal factors.

2.2 Current Legislation and Future Directives for the UTM in Brazil

Each sovereign State is responsible for its management and control, which includes its airspace. In Brazil, following the Código Brasileiro de Aeronáutica (CBA, law 7.565/1986), the Brazilian State performs the airspace control through the Força Aérea Brasileira, through its responsible department, the Departamento de Controle do Espaço Aéreo (DECEA) (Silva *et al.*, 2023).

The Instrução do Comando da Aeronáutica (ICA) 100-40 regulates access to the UTM airspace (Silva *et al.*, 2023). The ICA 100-40 provides all definitions and rules applicable for the UTM airspace access to permit drone operations such as agricultural, imaging, and information collection, among other types of unmanned aerial operations (DECEA, 2023).

The ICA 100-40 also defines the system to be used to request UTM airspace access as the Sistema para Solicitação de Acesso ao Espaço Aéreo Brasileiro por Aeronaves Não Tripuladas (SARPAS). Employing the SARPAS, the drone operator should introduce information related to the intended operation, such as the type of operation, drone model, responsible pilot, date, time, and location.

The Digital Airspace System Analysis (DASA) system, which is embedded in the SARPAS, is used to draw the location of the intended operation. The intended area of the operation is outlined in the DASA as an area on a map with a height limitation, thus generating a volume of airspace. The DASA compares if there are any restrictions on the intended volume of airspace, such as previous approved unmanned operations during the same period, intersections with Flight Restriction Zones (FRZ) of ATM airspace, and particular interest areas restrictions (e.g., military areas, borders, powerplants, etc.). If no restrictions are found, and the requested flight is within the allowable limits as per the ICA 100-40, the requested volume of airspace is granted automatically. If there are restrictions, for example, intersections with FRZ of airports or helipads, then the analysis is performed by a human analyst. In this case, an operational agreement with the operators of the affected airport or helipad will be required to approve the airspace request. Requests not complying with ICA 100-40

requirements may be denied (DECEA, 2023).

However, this process of analyzing and permitting or not access to the UTM airspace is not flexible and is already facing operational bottlenecks. For instance, a particular UTM airspace volume can be requested for up to 90 (ninety) days. During that period, the requester can perform only one or several flights or even not fly. If other operators want to fly in the same area, they will either have to reach an agreement with the one already operating in that area or wait until it is free. Another negative aspect of this process is that one operator can become a monopolist of a particular area of interest, which is undesired as it does not allow a free and open competitive market to flourish.

Figure 1 shows the number of UTM airspace requests per year in the SARPAS system since its launch in 2016. The graph shows continuous growth but does not reflect the number of flights. As a particular area can be requested for up to 90 days, an unknown number of flights can be performed during that time.

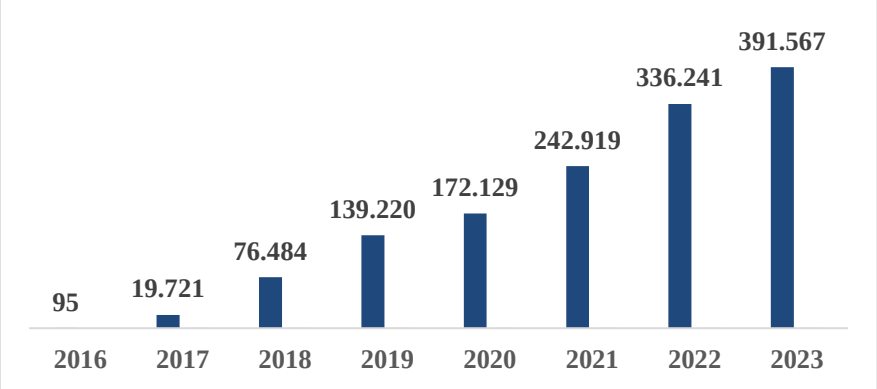


Figure 1 SARPAS UTM Airspace Requests per Year (2016-2023) (DECEA, 2024).

A new paradigm of airspace access and control must be established to permit a more efficient use of the UTM airspace. The Brazilian Aeronautical Command issued the Diretriz do Comando da Aeronáutica (DCA) 351-6 to reach that goal. This document provides directives on how to establish the UTM airspace, focusing on allowing an increasing number of unmanned operations of various types and several operational scenarios, from sparsely populated rural areas to densely populated urban areas and intersecting with the FRZ of ATM airspace (DECEA, 2022).

Among several innovations, the DCA 351-6 introduces the UAS Service Supplier (USS), allowing drone operations in a particular area. In summary, the USS will be a private entity that provides flight information services and flight permits to any drone operator who intends to fly in its area of operation. The underlying concept is that two or more USSs can provide services in the same location, allowing a competitive landscape similar to today for mobile phone operators (DECEA, 2022). This new paradigm presents several challenges, such as how to strategically and tactically separate drones operating in the same area (possibly with flight permits granted by different USSs) from each other and ATM airspace operations; how to precisely locate drones flying in a given area at all times; how to stop drone operations in case of an emergency such as a rescue mission, or a policing operation, among many more. A safety analysis using the STPA can help to identify hazards and provide safety recommendations for this new operational paradigm. The DCA 351-6 presents the concepts of the BR-UTM ecosystem, which is the Brazilian concept of operations applicable to the UTM airspace. A complete description of the BR-UTM can be found on the DCA 351-6, as it is beyond the scope of the present work.

3. METHODOLOGY

The methodology employed in this work consists of a case study. It utilizes the STPA method, uses the current legislation in Brazil concerning drone operations, and considers the directives that drive the implementation of the new paradigm of airspace control, specifically for drone operations.

The case study involves a package delivery operation from a shopping center to a residential condominium in the urban area of São José dos Campos/SP, Brazil. Using the AppSTPA tool, a preliminary STPA analysis is performed to find loss scenarios and safety recommendations for that operation from the airspace access and control viewpoint (Carniel, 2023).

To build the STPA case study, a simplified control structure of the UTM system was developed by the authors (described on Figure 4). As it will be further discussed in the Section 4, although the studied control structure is simplified, it is representative of the overall UTM system for a preliminary safety evaluation. A safety evaluation of a complex system is an iterative process that requires several cycles of the system design until a sufficient representation of the system is achieved, but not too complex that would cause the evaluation to be inconclusive.

The STPA, the current legislation and the future directives issued by the Brazilian aeronautical authorities, introduced in Section 2, were used as the theoretical foundation. Brainstorming sessions were used by the authors to define the UTM system control structure used in this case study.

Therefore, to the objective of the present work, only one element of the UTM system is considered, in contrast to the expected future system when several elements of each one will be operating simultaneously. Besides that, the control actions, feedback, process models, actuators and sensors are also simplified to keep to a minimum the UCAs, possible causal factors and associated safety recommendations.

4. RESULTS AND DISCUSSION

4.1 Case Study: Package Delivery in Urban Environment – Center Vale Shopping to Altos da Serra I Residential Condominium

A case study is presented to prepare an initial and preliminary STPA safety analysis of this new airspace access and control paradigm applicable to the UTM airspace. An analysis of the case of a package delivery from the Center Vale Shopping to Altos da Serra I Residential Condominium in São José dos Campos/SP, Brazil, is performed.

Figure 2 shows the drone path of the case study. It is an approximately 9 km path, from take-off to land, to be performed at 30 m height. The flight of the case study is a Beyond Visual Line-of-Sight (BVLOS) flight. Appropriate communication and control (C2) infrastructure should be available along the route. This will permit the Remote Pilot in Control (RPIC) to maintain two-way communication with the drone during operation and send commands if any abnormality occurs.

Figure 3 shows the DASA representation of the UTM airspace required for the intended operation. It shows intersections with seven manned aviation operators (one airport and six helipads):

- SBSJ (Professor Urbano Ernesto Stumpf) - Landing zone and internal horizontal surface of the airport.
- SJSW (Colinas Shopping) - Helipad.
- SIUJ (The One Office Tower) - Helipad.
- SJBS (São José dos Campos) - Helipad.
- SJCI (Capitão PM Paulo José de Menezes Filho) - Helipad.
- SJWM (Pátio das Américas) - Helipad.
- SWGR (Urbanova) - Helipad.

Per the current paradigm (ICA 100-40), the USS providing flight services and permits to that flight path would be required to establish operational agreements with all manned aviation operators intersecting with the drone operation. In a simplified explanation, the drone operator needs to develop two-way communication with each manned aviation operator to inform them whenever there is a drone operation. Conversely, each manned aviation operator has to notify the drone operator of each manned aviation operation in the area to avoid conflicts and possibly a crash between a drone and a manned aircraft.



Figure 2 Drone Path - Center Vale Shopping to Altos da Serra I Residential Condominium in São José dos Campos/SP, Brazil (Google Earth, prepared by the authors).

In the future, the BR-UTM ecosystem will automatically perform this deconfliction, providing ATM controllers with real-time situation awareness. The drones will count on a real-time tracking system that communicates with the applicable UTM services. That tracking information will be available to any other user of that volume of airspace, thus allowing the deconfliction to occur at a strategic level. The tactical deconfliction (drone collision avoidance system) will be necessary only in case of emergency, system failure, or error.

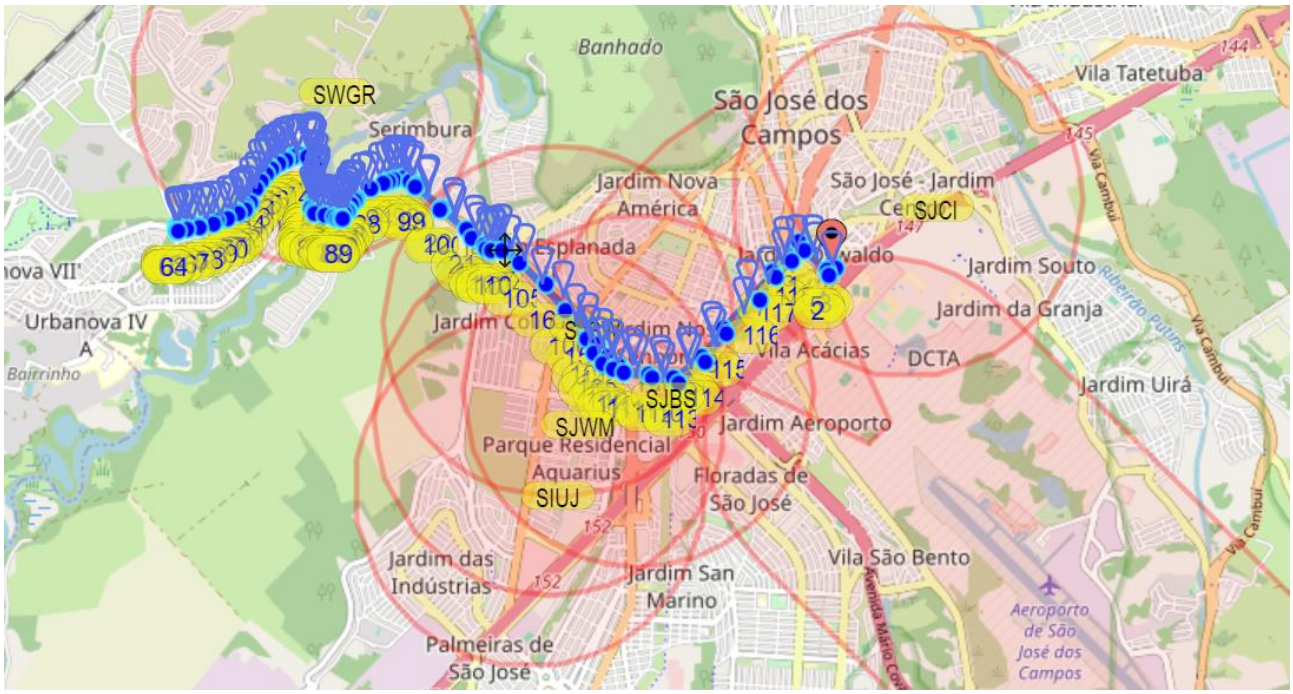


Figure 3 SARPAS/DASA Drone Path Showing Intersections with Manned Aviation (SARPAS, prepared by the authors).

4.2 STPA Preliminary Analysis – Usage of the AppSTPA Tool

A summary of the four steps required to perform the STPA analysis on the AppSTPA tool is described herein.

Step 1 requires the identification of the system goals, assumptions, losses, system-level hazards, and system-level safety constraints that define the purpose of the analysis. To perform Step 1, the AppSTPA tool does not provide any automated help to the analyst. The analyst records the losses,

hazards, and system-level safety constraints. The analyst must have previous knowledge of the system and the drone delivery scenario to perform that.

Step 2 draws the hierarchical control structure of the system under analysis (components, links, control actions, and feedback) (Leveson and Thomas, 2018). The AppSTPA tool requires that all system connections are identified and declared, following a process composed of 12 tasks. The tool uses the logic of ontology to verify what connections can be made by the control structure components to prevent mistakes and wrong connections and identify the type of links for the components (Carniel *et al.*, 2023). The elaboration of the system control structure proved a key step in the STPA analysis, especially in the concept stage, where the hierarchy and interactions between components are unclear. This step consumes considerable effort from the analyst. Figure 4 shows the system control structure considered in this case study.

Step 3 is the identification of the UCAs. A UCA is a control action that leads to a hazard in a particular context and worst-case scenario. To do this, the hazards identified in Step 1 and the control structure in Step 2, including the control action, are used. The type of issuance of control action and the context are used to determine if a control action is unsafe. The types of issuances of control actions are provided, not provided, provided too early, provided too late, provided in the wrong order, applied too long, and stopped too soon. The AppSTPA tool has a feature to build rules for unsafe control actions. The analysis of each type of issuance of control action in each context determines if a control action of a given controller is unsafe or not (Carniel *et al.*, 2023).

Step 4 is the identification of the loss scenarios. A loss scenario describes the potential causal factors that can lead to the UCAs and hazards (Leveson and Thomas, 2018). Step 4 also identifies the safety recommendations for each UCA identified in Step 3 (Carniel *et al.*, 2023).

4.3 STPA Preliminary Analysis – Results Obtained for the Case Study

The STPA analysis was performed using the AppSTPA tool. In total, the AppSTPA tool helped to identify a total of 20 UCAs (Step 3) and 206 possible causal factors with associated safety recommendations (Step 4). The complete report can be obtained by contacting the corresponding author. As an example, the safety analysis for the UCA-4 is described below:

UCA-4: DRONE EMBEDDED CONTROLLER provided Release Package at Destination when Package Presence is YES, Location is NOK. This UCA means that the package is released in the wrong location. It is linked to the following hazards:

- H-1: Drone flying close to persons.
- H-2: Drone flying close to third-party property.
- H-3: Drone flying outside of its flight permit (4D, time and location).
- H-5: Persons at/near the droneport when the drone is operating.
- H-7: Package released outside of destination place.

A total of 24 possible causes were identified by the analysis, with associated safety recommendations for that UCA. Examples of potential causes identified by AppSTPA include:

- Incorrect drone controller algorithm/logic.
- Improper drone controller algorithm/logic update.
- Component specification/precision improperly designed.
- Communication failure among system actuators, sensors, and controllers.
- Component failure, lack of proper maintenance, and out-of-range sensors.

The possible causes identified by the tool are linked to the following safety recommendations:

- Assure that the controller algorithm/logic is implemented correctly and is properly tested before field implementation, including software updates.
- Assure component specifications are designed and tested in realistic scenarios.
- Implement redundant communication among system actuators, sensors, and controllers.
- Assure an effective maintenance plan is in place to detect failed components or out-of-range sensors.

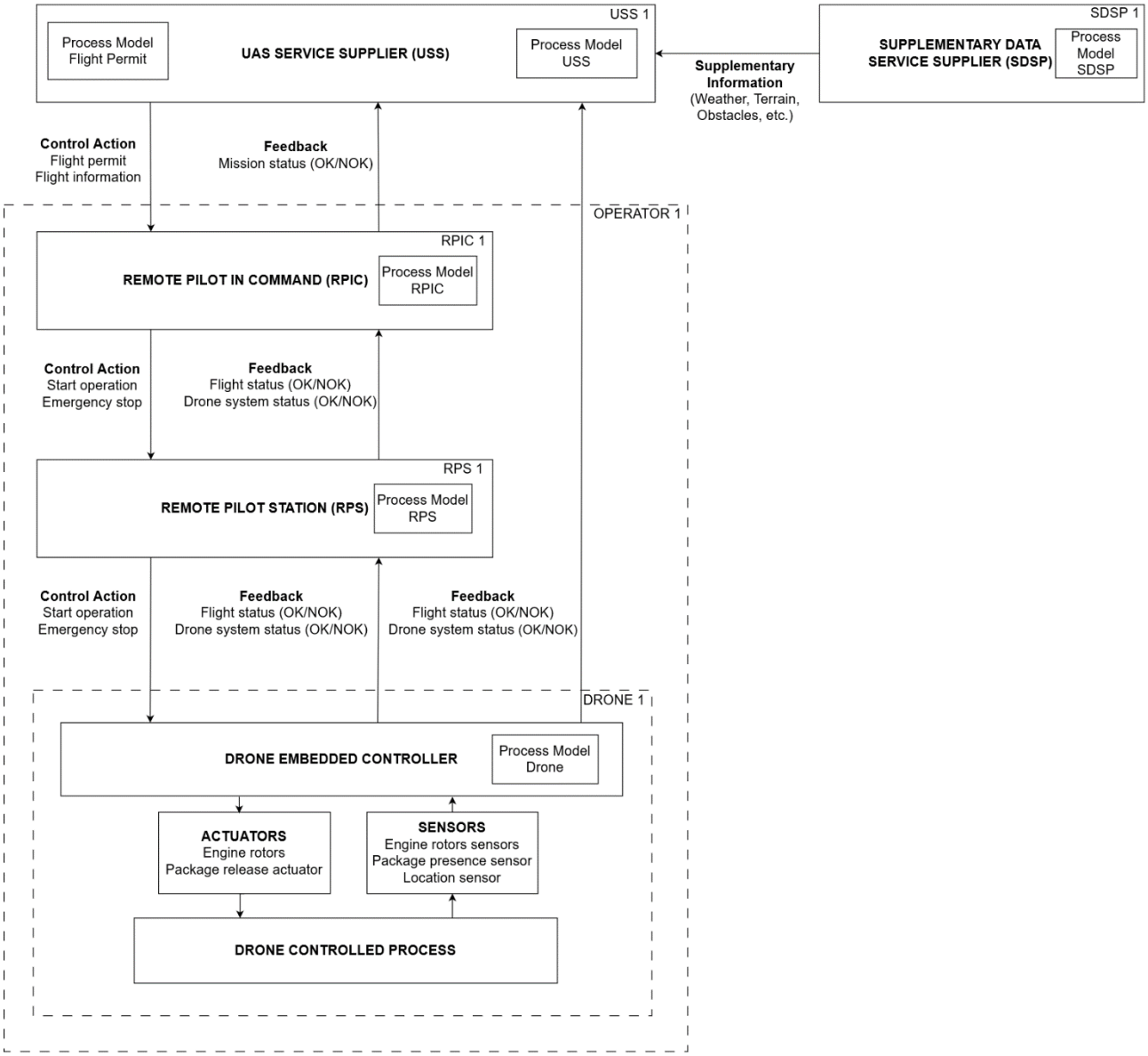


Figure 4 System Control Structure Considered in the Case Study (prepared by the authors).

The AppSTPA helped to identify a wide range of possible causes and safety recommendations related to the specific system under analysis. It also helps drive the system architecture, create requirements, identify mitigations and safeguards, define tests and maintenance requirements, evaluate design decisions and safety gaps, develop leading safety indicators, and ultimately lead to a more effective overall system design (Leveson and Thomas, 2018). The tool also permits the analyst to evaluate possible mechanisms to meet the safety recommendations. However, this task was not performed in the present work as it is beyond the proposed scope. The tool generates several possible causal factors and associated safety recommendations. A substantial quantity is repetitive since the causal factors are common in many loss scenarios. An enhancement of the tool is required.

5. CLOSING REMARKS

5.1 Limitations of the Work and Suggestions for Future Works

The present work is a preliminary safety assessment that requires further review from industry stakeholders and safety experts. This analysis requires constant reviews and updates as new hazards are identified, assumptions can change, and loss scenarios that were not previously identified can

occur.

The system control structure is simplified compared to the complete concept of operation of the BR-UTM ecosystem. For example, only one element of each system component was included in the analysis (one USS, one Operator, one RPIC, one drone, etc.), with the consequence that no hazards linked to drone-to-drone interferences were analyzed. The analysis did not consider interactions with manned aviation and State Security Forces.

Therefore, future work suggestions would be to expand the control structure to include more than one element of each system component, include assessments of other industry experts, include interactions with manned aviation and State Security Forces, and compare real-life cases with theoretical results obtained by the presented methodology.

5.2 Conclusions

The preliminary assessment presented in this work showed that the STPA is a robust methodology for performing a safety analysis of the UTM system since its early development stages. With the aid of the AppSTPA tool, a comprehensive analysis of safety-critical systems could be conducted to identify unsafe control actions, hazards, loss scenarios, and safety recommendations. As discussed in the AppSTPA tool usage analysis, the model of a control structure is a critical step that consumes considerable effort; however, it is fundamental for the results of the STPA analysis.

The delivery of packages in an urban area using drones is a foreseeable application for the UTM system. The system requires a safety analysis to be performed since its early development stage. With the use of the STPA method and the AppSTPA tool, a complete system analysis was possible.

The tool helped identify 20 unsafe control actions and 206 possible causal factors with associated safety recommendations. Therefore, the objective of the proposed work was reached: to perform a preliminary assessment of hazards, unsafe control actions, possible causes, and safety recommendations of the package delivery mission with the use of drones in a densely populated urban environment.

6. REFERENCES

Agência Nacional de Aviação Civil (ANAC). (2023). *RBAC-E Nº 94 – Requisitos Gerais para Aeronaves Não Tripuladas de Uso Civil – Emenda 03*. [Online]. Available: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94. Accessed: Dec. 27, 2023.

Carniel, A., Bezerra, J. D. M. and Hirata, C. M. (2023). An Ontology-Based Approach to Aid STPA Analysis. *IEEE Access*, vol. 11, pp. 12677-12697. DOI: https://doi.org/10.1109/ACCESS.2023.3242642.

Carniel, A. (2023). *GitHub Repository of AppSTPA*. [Online]. Available: https://github.com/andrei-carniel/AppSTPA. Accessed: Dec. 27, 2023.

Departamento de Controle do Espaço Aéreo (DECEA). (2022). *DCA 351-6 – Concepção Operacional UTM Nacional*. [Online]. Available: https://publicacoes.decea.mil.br/publicacao/DCA-351-6. Accessed: Dec. 21, 2023.

Departamento de Controle do Espaço Aéreo (DECEA). (2023). *ICA 100-40 – Aeronaves não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro*. [Online]. Available: https://publicacoes.decea.mil.br/publicacao/ica-100-40. Accessed: Dec. 21, 2023.

Departamento de Controle do Espaço Aéreo (DECEA). (2024). *SARPAS Em Números – Informativo Trimestral – Abril a Junho/2024*. [Online]. Available: https://www.decea.mil.br/static/uploads/2024/07/Informativo_trimestral_SARPAS_02_2024-_abr_jun_corrigido-1.pdf. Accessed: Aug. 5, 2024.

Drone Industry Insight. (2023). *Drone Market Report 2023-2030*. [Online]. Available: https://droneii.com/product/drone-market-report. Accessed: Jan. 3, 2024.

International Civil Aviation Organization (ICAO). (2023). *Unmanned Aircraft Systems Traffic*

Management (UTM) – A Common Framework with Core Principles for Global Harmonization – Edition 4. [Online]. Available: https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%204.pdf. Accessed: Jan. 25, 2024.

Leveson, N. G. and Thomas, J. P. (2018). *STPA Handbook*. Cambridge, MA, USA: MIT Press. [Online]. Available: http://psas.scripts.mit.edu/home/materials/. Accessed: Jan. 16, 2024.

Plioutsias, A., Karanikas, N. and Chatzimihailidou, M. M. (2018). Hazard Analysis and Safety Requirements for Small Drone Operations: To What Extent Do Popular Drones Embed Safety? *Risk Analysis*, vol. 38, pp. 562-584. DOI: https://doi.org/10.1111/risa.12867.

Silva, E. A., Rosa, C. E. V., Rainho, J. H. V. (2023). O uso irregular dos drones: Breves apontamentos à luz da responsabilização administrativa, penal e civil. *Direito Aeronáutico*, vol. 3, 1ª ed., pp. 781-792. Belo Horizonte, São Paulo: Ed. D'Plácido.