https://doi.org/10.1590/jatm.v18.1426 ORIGINAL PAPER

A Method for Eliciting Safety Requirements for Military Unmanned Aircraft Systems Related to Critical Scenarios

Douglas Estevam Casale[1,*], Rafaela Campos da Silva[1], José Tupinambá Lopes Viana Júnior[2], Moacyr Machado Cardoso Junior[1], Luís Eduardo Vergueiro Loures da Costa[1]

1. Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – São José dos Campos/SP – Brazil.
2. Departamento de Ciência e Tecnologia Aeroespacial – Instituto de Fomento e Coordenação Industrial – Divisão Certificação de Produto Aeroespacial – São José dos Campos/SP – Brazil.

***Corresponding author:** casale.douglas@gmail.com

ABSTRACT

The expansion of unmanned aircraft systems (UAS) usage has highlighted the need for robust safety mechanisms to mitigate operational risks in critical scenarios. In this context, it is envisioned that the potential of the critical decision method (CDM), a semi-structured interview technique that utilizes non-routine incidents to capture the decision-making processes employed in these situations and explore how different actions might have influenced the outcome, can be used to elicit knowledge that will contribute to safe UAS operation. However, there is a gap in the literature concerning the proposals and guidance for utilizing CDM in the systems development requirements elicitation process. This study aims to address this gap by applying CDM combined with model-based systems engineering to systematically elicit the safety requirements for UAS in critical operational scenarios. The methodology involves stakeholder interviews, scenario analysis, and requirements elicitation that reflect both operational insights and situational hazards. Sixty-eight safety requirements were identified for the UA and 51 for their ground control stations, providing a comprehensive framework for enhancing safety. The study concludes that CDM is an effective tool for eliciting requirements, offering significant contributions to the early design phases of UAS projects and supporting the development of safer and more resilient systems.

Keywords: Unmanned aircraft systems; Flight safety; Safety factors; Critical decision method; Human factors; Systems engineering.

INTRODUCTION

Unmanned aircraft systems (UAS) consist of three primary components: the unmanned aircraft (UA), the ground control station (GCS), and the command and control link (C2 link) connecting them. The widespread adoption of UAS across sectors such as logistics (Avelino *et al.* 2023), agriculture, wildfire monitoring, disaster response, industry, and defense (Casale *et al.* 2025) has opened diverse application opportunities.

Although the lower mass of UAS reduces the risk of typical aviation accidents such as runway overruns (Reiser *et al.* 2024), their operational versatility (Tostes *et al.* 2025) and capacity to undertake hazardous missions without endangering human lives (Gupta *et al.* 2021), their reliance on sensor fidelity for tactile, vestibular, and visual inputs introduces operational challenges, that are further exacerbated by the mental load imposed on UA pilots (Russo *et al.* 2025) and the inability to disable or minimize automation when necessary (Grindley *et al.* 2024). Automation, while beneficial, has been criticized for degrading operator situational awareness and response effectiveness, even contributing to fatal incidents (Hart *et al.* 2022).

Received: Aug. 04, 2025 | **Accepted:** Dec. 18, 2025
Peer Review History: Single Blind Peer Review.
Section editor: Renato Reboucas de Medeiros

Moreover, the low cost, ease of acquisition, and difficulty in supervising and controlling individual UA operations raise safety concerns, including system failures, mid-air collisions, ground impacts (Du *et al*. 2024), and incidents involving construction workers (Karakhan and Al-Mhdawi 2024). To address these risks, UAS must embed intrinsic safety mechanisms that function not only under normal conditions but also in degraded and unforeseen scenarios. Identifying such critical situations, understanding their dynamics, and defining appropriate system responses are key steps toward safe operation in complex environments.

Requirements engineering (RE) offers a structured approach to address these challenges throughout the system lifecycle. By capturing both functional and non-functional aspects, RE supports the identification, monitoring, and validation of system characteristics, including safety (Dick *et al*. 2017) and environmental risk mitigation (Subahi 2023).

Several elicitation techniques exist, such as interviews (Dar *et al*. 2018), questionnaires, fuzzy logic (Akram *et al*. 2024), non-functional requirement frameworks (Saxena *et al*. 2024), use cases, and design thinking (Kahan *et al*. 2024). However, these methods often face limitations in capturing the decision-making complexities of dynamic, high-stakes environments such as UA operations. Accurately eliciting safety requirements under such conditions demands a deeper understanding of how operators make decisions in uncertain and time-constrained scenarios.

One promising yet underexplored method is the critical decision method (CDM). Developed by Gary Klein in 1989 within the field of naturalistic decision making (NDM), CDM was designed to explore expert decision-making in real-world, complex, and high-pressure situations (Hoebbel *et al*. 2024; Klein *et al*. 1989). Unlike classical models that assume rational and sequential decision processes, NDM emphasizes rapid, experience-based judgments under uncertainty, recognizing patterns and acting quickly, which are common in fields such as military operations (De Carvalho Lourenço & Cardoso-Júnior 2025), firefighting, and emergency medicine.

The CDM is a semi-structured interview technique that explores how people navigate non-routine situations. Its five steps are:

- Selection of a non-routine incident where experience influenced the outcome.
- Elicitation of the actor's account with minimal interviewer interference.
- Timeline construction to clarify gaps or ambiguities.
- Identification of decision points where actions affected the outcome.
- Investigation of cues, goals, and knowledge behind each decision point, including questions used as probes to better understand the strategies to make decisions.

The use of CDM expanded over time. For example, Mansikka *et al*. (2024) trained instructors to use CDM during the debriefing of upgrade pilots' flight combat training. They concluded that this approach facilitated a deeper understanding of the processes and knowledge underlying learners' decisions, rather than focusing solely on outcomes, which can sometimes occur by chance. This process-oriented focus enhanced trainees' situational awareness and overall performance.

Specifically, to support the process of gathering information for requirements elicitation, Asmayawati and Nixon (2020) applied CDM as a knowledge elicitation technique and used it to propose seven design recommendations about how technology should automate actions or display information to the crew. In turn, these design recommendations are a source of requirements to be refined and implemented in the system at appropriate levels.

Klinger and Gomes (1993) described the use of CDM in association with concept mapping (a diagram for representing important relationships among concepts and ideas) to propose modifications to software features and improve user interfaces, and thus, operator performance.

Hoebbel *et al*. (2024) interviewed haul truck operators following the CDM guidelines to identify emergent decision-related themes that may impact the outcome of non-routine and critical situations, for example, to avoid the loss of human life, The most prevalent themes found in this study were "know your truck," "safety first," and "situational awareness," pointing to a possible direction for improvement to reduce the accident rate and preserve the workers. In this work, the authors do not elicit requirements but state that the results can reveal hidden hazards and create requirements for training scenarios, making them closer to reality.

Cattermole *et al*. (2016) went a little further and based on CDM interviews with officers experienced in response to traffic incident management (TIM) tasks. The authors identified interface requirements among agencies participating in TIM, resource requirements (such as changing color lights), training requirements, and process requirements.

The CDM's semi-structured nature supports a transparent and consistent data collection process (Plant and Stanton 2016). As demonstrated in the literature, the CDM offers a systematic means of studying and understanding critical scenarios, which can provide a robust foundation to support the identification of safety requirements. However, despite its versatility and the insights it can generate, there remains a notable gap in the literature concerning proposals and guidance to systematically translate these insights, derived from CDM application, into formal safety requirements that can be directly integrated into system design, considering both experienced and probable scenarios.

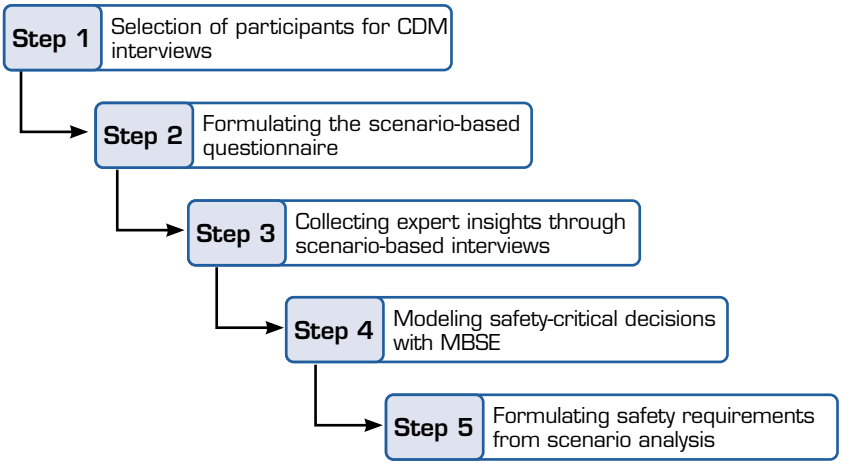
In this regard, model-based systems engineering (MBSE) can enhance the definition of safety requirements by structuring CDM information into diagrams that map decision points, scenario-specific risks, and expected system responses. MBSE is an approach that uses models, simplified representations of reality or concepts, to support system development (International Council on Systems Engineering [INCOSE] 2021) and was proposed to enhance the capture, analysis, sharing, and management of information, aiming to integrate the multiple project domains in a single environment (Friedenthal *et al.* 2007). It improves system behavior visualization, facilitates stakeholder comprehension, and ensures the seamless integration of safety requirements into system architecture, which may contribute to a shared view and better understanding of the project and identification of the functions of the system of interest (SoI), that is, the system currently under development (Douglass 2016). Additionally, when using MBSE software, these diagrams can be incorporated into the system model, enhancing traceability and completeness

This study proposes an integrated approach to support the elicitation of safety requirements for UAS in critical operational scenarios that combines CDM and MBSE. It is important to emphasize that the focus is not on general safety requirements but on identifying and extracting scenario-specific safety requirements, thereby contributing to a deeper understanding of the safety needs of UAS operations, complementing traditional safety requirement elicitation methods, and thus enhancing the reliability and safety of UAS operations.

Whereas CDM facilitates a structured analysis of scenario-related decision points, cues, and alternatives, MBSE enhances the analysis and sharing of information, thereby improving the safety requirements elicitation process for the selected scenarios. To the best of the authors' knowledge, no prior studies have applied CDM to product development, particularly for hardware defense systems, nor have they combined CDM with MBSE in this context. Thus, this work likely represents a novel application of these theoretical models.

METHODOLOGY

To identify safety requirements for specific UAS operational scenarios, this study proposes a five-step method, as summarized in Fig. 1.



Source: Elaborated by the authors.

Figure 1. Diagram representing the five-step method for this paper.

Step 1: selection of participants for CDM interviews

The first step involves identifying key participants who will participate in CDM interviews. These individuals serve as primary sources of information on critical events, providing essential insights into the operational context, potential challenges, and decision-making processes in real-world scenarios that contribute to the identification of safety requirements. Suitable participants include experts, operators, maintainers, and technicians, whose experience ensures a comprehensive understanding of the system's operational landscape.

Step 2: formulating the scenario-based questionnaire

This step involves formulating a structured questionnaire to identify critical scenarios and extract essential information. The first activity is to identify the operational scenarios where operational safety risks may arise, through an analysis of the concept of operations of the system (describing the operational environment, the mission profiles, the system interactions and constraints), analysis of historical data from previous incidents, accident reports, and safety bulletins from UAS operations in similar domains, and expert consultation. If an excessive number of scenarios are identified, they should be prioritized based on their relevance, discarding those with low operational impact. Klein designed CDM for time-constrained interviews, sometimes as brief as 15 minutes. While this represents an extreme case, keeping interviews concise enhances engagement and ensures meaningful data collection. After that, for each selected scenario, the team shall create a structured set of CDM-based questions to explore:

- Diagnosis: how does an expert recognize the occurrence of the problem? What cues and signals indicate it?
- Consequences and complicating factors: what are the potential impacts and elements that worsen the situation?
- Intervention strategies: how do operators respond to mitigate risks?
- Alternative and preventive actions: what measures can be taken to mitigate or avoid the issue?

The development of interview questions is guided by the CDM, which suggests probes to elicit situational cues and decision points. To enhance question design, it is recommended to consult the Joint Authorities for Rulemaking of Unmanned Systems (JARUS) Specific Operations Risk Assessment (SORA), a methodology for assessing the risk and safety requirements of UAS operations (including those related to the system, operator, and training) (JARUS 2024). The SORA is adopted in several countries, including those under the European Union Aviation Safety Agency (EASA), as well as Canada, Australia, Indonesia, and Namibia, and is being implemented in Brazil to revise Brazilian Civil Aviation Regulation (Regulamento Brasileiro de Aviação Civil [RBAC]) 94 and introduce RBAC 100. Finally, pilot testing with stakeholders is recommended to refine the questionnaire before full implementation.

Step 3: collecting expert insights through scenario-based interviews

In this step, CDM-based interviews are conducted with UAS experts to gather in-depth insights on how they recognize, interpret, and respond to hazardous operational scenarios. To optimize time, participants should first indicate which scenarios they are familiar with, as they may not feel confident discussing all of them.

Following CDM principles, interviews begin with minimal interviewer intervention, allowing participants to describe the incident freely while the interviewer takes notes. Once the initial account is complete, clarifying questions shall be asked to ensure that all critical elements of the scenario are covered, including:

- Cues and indicators that signaled the onset of the hazard.
- Complicating factors that made the response more challenging.
- Decision points where actions should be taken based on available information.
- Consequences of the decisions, assessing whether they solved the problem or led to further complications.
- Alternative strategies considered, their rationale, and their potential to improve decision-making or system automation.
- Preventive actions that could have reduced the likelihood or severity of the incident.
- As prescribed in the CDM technique, to enhance the accuracy and completeness of expert accounts, interviewers should create a handwritten timeline during the interview, mapping key moments in sequential order. This allows for immediate validation and refinement of information, ensuring consistency and reducing recall errors. Additionally, this approach helps identify

patterns in expert decision-making, revealing system functions that could be automated, opportunities to replace operator interventions, and the parameters required to determine the best course of action in each situation.

To keep interviews dynamic, the questionnaire should serve as a guide, not a strict script. If a participant has already addressed certain questions or if some become irrelevant due to the context provided, they can be skipped to maintain a natural flow.

Step 4: modeling safety-critical decisions with MBSE

To transition from qualitative insights to MBSE diagrams, the development team shall highlight decision points (moments where the actor had multiple action options) along with the associated cues, goals, situational assessments, available options, and influencing knowledge. This analysis helps clarify the decision-making process and rationale and ensures that expert-driven knowledge is traceable throughout the system architecture. Examples of diagrams that can be useful for this step are:

- Use Case Diagrams: mapping interactions between components, operators, and external factors in hazardous scenarios.
- Activity Diagrams: representing workflows and decision sequences, ensuring expert strategies are systematically modeled.
- State Machine Diagrams: defining system transitions based on triggers such as sensor failures or loss of communication.
- Sequence Diagrams: illustrating how information flows within the system in response to critical events.

These diagrams allow engineers to validate and refine decision-making processes and decisions from experienced operators extracted from CDM. The choice of diagrams depends on the system characteristics the team wants to represent, while the selection of the MBSE software depends on the development environment, ensuring integration with the product model.

Step 5: formulating safety requirements from scenario analysis

This step aims to integrate the information gathered from interviews and MBSE diagrams to elicit a comprehensive set of safety requirements. These requirements define the functions, behaviors, features, characteristics, and properties of the SoI, ensuring its ability to navigate hazardous scenarios while mitigating risk.

The CDM analysis will contribute to the elicitation of the requirements. The identification of "cues" highlights critical aspects that must be monitored to detect hazardous conditions. These insights guide sensor selection and interface design requirements, ensuring that the system can recognize early warning signs and effectively alert operators. Similarly, the "decision points" identified during interviews indicate specific situations where the system must perform certain functions based on expected behaviors and expert-recommended solutions. These insights inform the definition of automated responses, control logic, and fail-safe mechanisms. Furthermore, "complicating factors" represent barriers or risks that the system must address to maintain functionality in hazardous environments. These factors emphasize the need for robustness and redundancy requirements. In addition, "alternative" and "preventive actions" suggest resilience measures that enhance system reliability and failure recovery, translating into contingency planning.

Whereas CDM provides the expert-driven foundation, MBSE offers a structured framework to refine and formalize system behavior, enhancing its visualization. Use Case Diagrams define system-level safety functions by mapping interactions between UAS components, operators, and external entities. These diagrams help identify responsibilities, decision points, and required safety functions. For instance, if a use case diagram illustrates that an operator must manually intervene to avoid obstacles, this may suggest the need for automatic collision-avoidance capabilities. Sequence Diagrams highlight the sequence of measures during UAS operation, clarifying component interaction and their interfaces. State Machine Diagrams provide insights into different modes of operation for handling critical scenarios and the conditions that trigger transitions between these modes.

To formalize the writing of the requirements, ensuring clarity and consistency, it is suggested to follow established standards and guidelines, such as ISO/IEC/IEEE 15288 (2023). For example, Carson (2015) proposes the following boilerplate:

The <AGENT> shall <WHAT> <HOW> <UNDER WHAT SITUATIONS>

The <AGENT> is the stakeholder, system, subsystem, component, or other. The verb "shall" indicates the requirement as mandatory. <WHAT> is the action or characteristic, <HOW> is the property or the level of performance needed, and <UNDER WHAT SITUATIONS> indicates environmental conditions, states, modes, and properties when the requirement applies.

For example, if multiple operators report that sensor failure indications are difficult to detect, a requirement may be formulated as "The UAS shall provide a visual and auditory alert when sensor accuracy deviates by more than 10%."

Finally, it is proposed to analyze the complete set of safety requirements, to solve eventual conflicts among requirements through negotiation with stakeholders, and to check characteristics such as completeness, feasibility, alignment, and consistency. Some of them, such as the completeness of the set of requirements, are very challenging to guarantee in practice, as there are some factors in the project that people do not know they ignore (the so-called "unknown-unknowns") (Larson *et al.* 2009). This analysis plays an important role in improving the quality of requirements, because the cost of addressing errors detected later in the project lifecycle increases significantly as the project progresses (Iqbal *et al.* 2020)

RESULTS AND DISCUSSION

This section applies the proposed method to elicit military UAS safety requirements in critical scenarios using CDM in stakeholder interviews.

Step 1: selection of participants for CDM interviews

To select participants for the CDM interviews, the authors identified individuals with experience in UAS maintenance, operation, engineering, and certification. The lead author personally consulted selected participants, while additional experts were identified at UAS and technology symposiums, expanding the initial pool.

A total of 11 experts agreed to participate, with experience ranging from 3 to 8 years, with a mean of 6.36 years (standard deviation [SD] = 1.57). Their mean age was 36.18 years (SD = 6.6), ranging from 28 to 48 years. The relatively low average experience reflects the recent integration of UAS into their organizations.

Step 2: formulating the scenario-based questionnaire

Five critical scenarios were identified by authors' consensus (Table 1) and were validated through participant feedback during the interviews. This number maintained the feasibility of the interview process, with no exclusions required. Scenario-specific questions were then developed using CDM probes to clarify ambiguities in participants' descriptions of real or hypothetical events, identify decision points, and elicit elements of NDM. Questionnaires were pilot tested to ensure clarity, relevance, and effectiveness. The criticality of some scenarios is context-dependent. For instance, GNSS signal loss, which can be caused by ionospheric phenomena (Rodrigues *et al.* 2022), is more severe in automatic operations than in those allowing manual override. Likewise, communication loss always degrades safety but may not result in hazardous outcomes; for example, C2 link failure is more critical in manual than in automatic operation.

Table 1. Critical scenarios and motivation.

Scenario	Description	Motivation
1	Hazardous environmental conditions, e.g., severe weather, electromagnetic interference without total loss of communication, etc.	This scenario can impair sensor accuracy, reduce maneuverability, degrade UAS performance, or precede a communication loss.
2	Communication loss	This scenario directly affects the ability to control the UAS and receive telemetry data.
3	Global Navigation Satellite System (GNSS) signal loss	This scenario impacts UAS's ability to navigate accurately and execute the mission task.
4	Power failure, e.g., sudden power failure, engine failure, or critically low battery during flight	This scenario can lead to the UAS becoming uncontrollable and colliding with other aircraft or crashing in sensitive areas with people, animals, or property.
5	Mechanical failure caused by collision, system malfunction, or other reasons	This scenario can lead to the UAS becoming uncontrollable and colliding with other aircraft or crashing in sensitive areas.

Source: Elaborated by the authors.

Step 3: collecting expert insights through scenario-based interviews

This section presents some of the key insights obtained from the CDM interviews, highlighting critical challenges and risk mitigation strategies identified by experts in UAS operations.

The interviews revealed that a significant concern in UAS operations is the ability to adapt to changes in the flight plan during a mission. These changes often arise when stakeholders request additional missions or when operational circumstances necessitate altering the area of operation.

In crewed aircraft, pilots manage unforeseen situations by following established procedures while adapting to dynamic conditions, weighing outcomes, and maintaining flexibility. This human adaptability enables nuanced prioritization and decision-making. Whereas UAS operations can similarly benefit from operator flexibility during direct control, this advantage is lost during communication link loss, leaving the UAS dependent solely on pre-programmed routes and onboard logic.

The dynamic nature of certain UAS missions often requires rapid redeployment to new areas of interest, sometimes before a detailed flight plan or return route analysis can be completed. Urgent mission updates or directives from authorities may prompt immediate action, even before emergency landing areas or safe return paths are identified. In such cases, operators typically redirect the UAS and only then begin assessing terrain features and constraints, such as population density. Safety in these contexts hinges on effective operator involvement, either through real-time control or through preemptive planning to avoid threats, restricted zones (e.g., airports), and to define safe flight paths within the operational area. The challenge arises when a communication link is lost before all contingency plans are in place, leading to hazardous scenarios.

For example, if a UAS initiates a "Return Home" routine without accounting for terrain elevation, it risks controlled flight into terrain (CFIT) or entry into restricted areas. Similarly, in the event of a sudden mechanical failure, the absence of pre-identified emergency landing zones may lead the UAS to crash in populated areas. Some systems mitigate CFIT during return routines using obstacle-avoidance sensors or by automatically climbing 2,000 feet before navigating back. While effective in Class G airspace (uncontrolled), such maneuvers may breach separations in controlled airspace, underscoring the need for further analysis to balance mitigation strategies with potential new risks.

Across the five critical scenarios, common mitigation strategies were identified, with the optimal response dependent on situational data. Interview analysis revealed that implementing distinct UAS operational modes adds a safety layer, as critical scenarios often emerge abruptly. Defining general response patterns, such as enabling manual override or triggering pre-programmed actions like returning, landing, or diverting to a crash site, simplifies system design and enhances operational resilience.

Step 4: modeling safety-critical decisions with MBSE

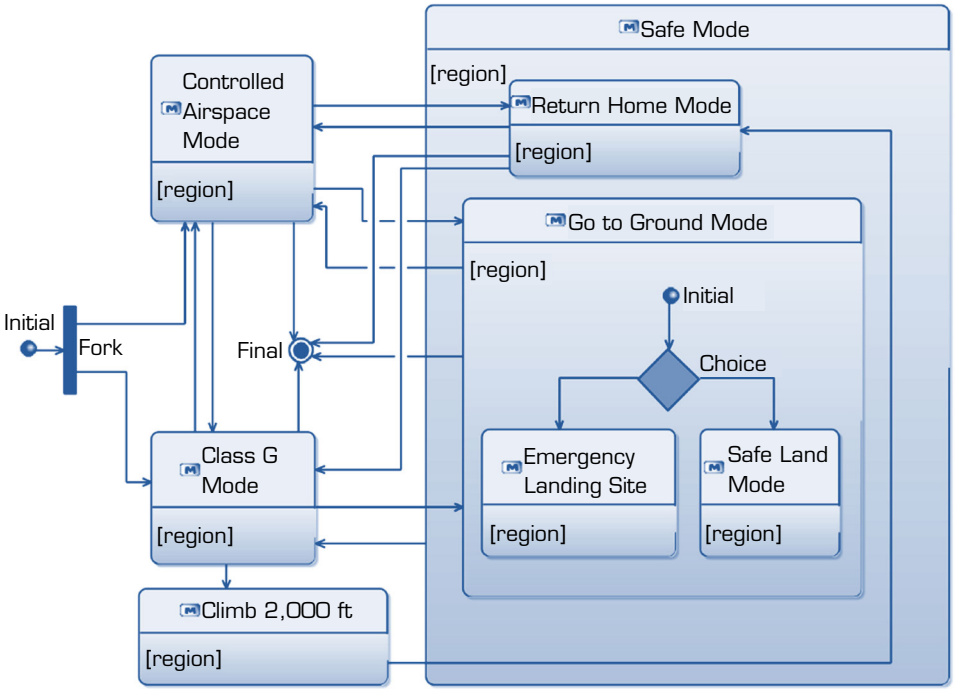
To enhance the visualization of UAS behavior in the selected critical scenarios, the authors developed MBSE diagrams based on interview data. The following discussion presents key insights derived from the interviews and their contribution to understanding system responses and informing design strategies.

Basic modes of operation, alternatives to finish the mission, and mitigate risk for all scenarios

Airspace classification plays a key role in selecting appropriate risk mitigation strategies for critical scenarios. Adaptive operational modes tailored to environmental and situational conditions can improve risk management. Two primary modes were defined: "Class G Mode" and "Controlled Airspace Mode." The main distinction lies in altitude management, as Class G Mode allows the UA to climb before returning home to avoid terrain obstacles, whereas Controlled Airspace Mode restricts climbing to prevent intrusion into helicopter traffic zones. This distinction reflects differing operational contexts: military missions often operate beyond visual line of sight (BVLOS) in Class G airspace, whereas police operations are typically VLOS within urban areas.

In the event of system failure, both modes may transition to a "Go to Ground Mode," directing the UA to a mapped emergency landing site (typically an uninhabited area) or to perform a safe landing (when, for some reason, an emergency landing site is not reachable, due to an aerodynamic surface breakage, for example). If the UA remains controllable with sufficient battery, it may enter "Return Home Mode," as illustrated in the State Machine Diagram (Fig. 2), developed using the open-source Capella tool.

The decision among options relies on sensor data and the UA's ability to return or reach a safe landing site. Following the RE method, this step aims to identify the high-level behavior of the system. It is not the objective of this step to define the solutions

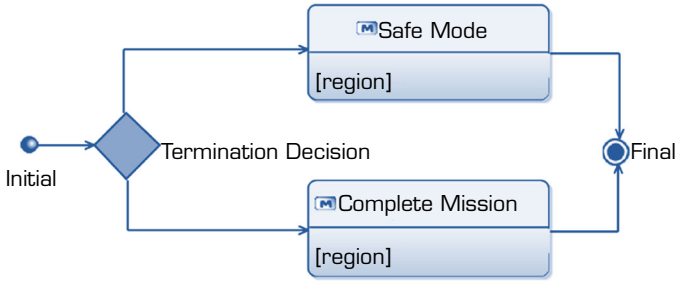


Source: Elaborated by the authors.

Figure 2. Basic operational modes State Machine Diagram for the UA.

or components associated with each decision, or to develop a low level of abstraction logic behind the software that will later be coded to implement the functions, although some high-level features and characteristics are cited, coherent with the dominant conception approach (Mendes 2018).

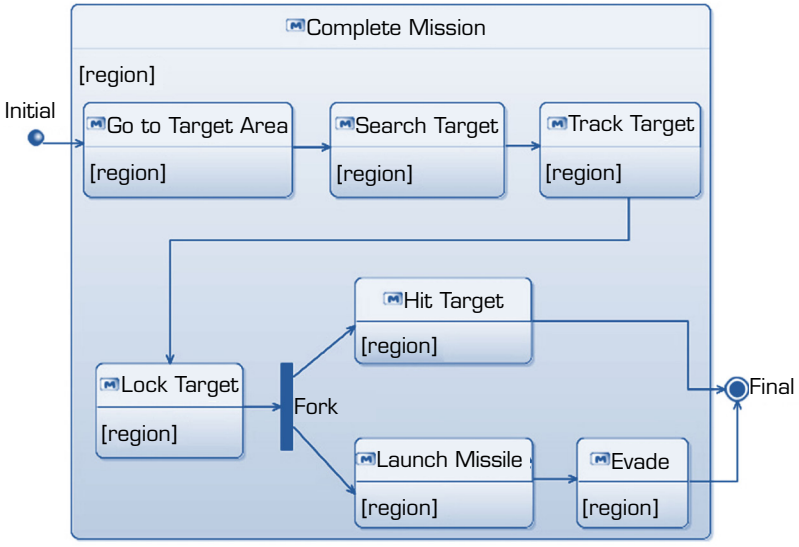
Military UAS faces additional challenges, as mission success may take precedence over minimizing risk. This requires the aircraft to execute pre-programmed tasks and engage targets despite adverse conditions or deceptive interference from opposing forces, even in cases of communication or GNSS signal loss. This behavior is implemented by the "Finish Mission" State Machine Diagram, presented in Fig. 3.



Source: Elaborated by the authors.

Figure 3. Finish Mission State Machine Diagram, presenting a decision between two modes of operation, based on decision factors.

Figure 4 illustrates the "Complete Mission" mode, outlining a high-level process for target engagement within a structured operational framework. The sequence begins with navigation to the designated target area, followed by target search, identification, and tracking. Once the target is locked, engagement proceeds: loitering munitions strike the target directly, whereas other UAS may launch a missile. In the second case, the system automatically initiates post-engagement evasive maneuvers to protect the platform.



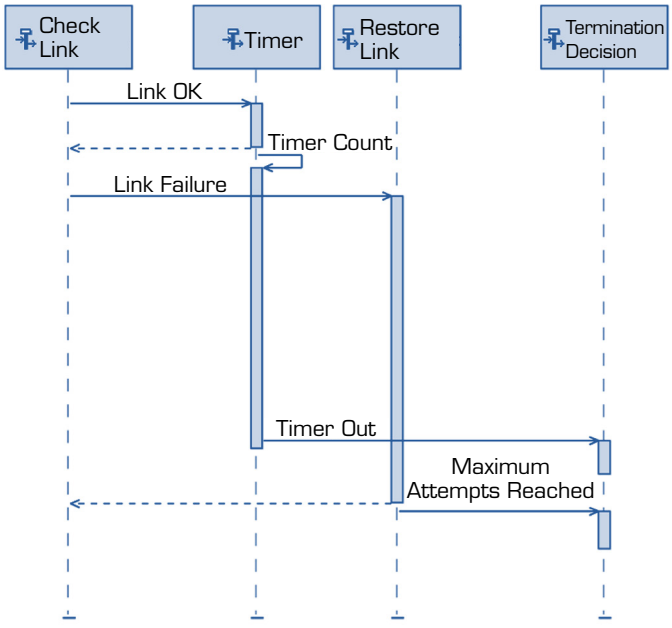
Source: Elaborated by the authors.

Figure 4. Complete Mission State Machine Diagram for the UA.

Scenarios 1 (hazardous environmental condition) and 2 (link loss)

Total link loss can occur either abruptly or because of progressive degradation due to environmental factors, interference, or unavailability of external services (e.g., cellular or satellite networks). Thus, scenarios 1 and 2 were identified as closely related situations that could be addressed within the same Sequence Diagram.

Operating within VLOS reduces the likelihood of link loss, but BVLOS missions may be required, increasing this risk. Typically, link degradation occurs gradually, prompting operators to guide the UA toward areas with a stronger signal, or the UA can be programmed to fly circuits in an attempt to restore the connection. Throughout this process, the UAS automatically monitors the link status, as illustrated in Fig. 5.



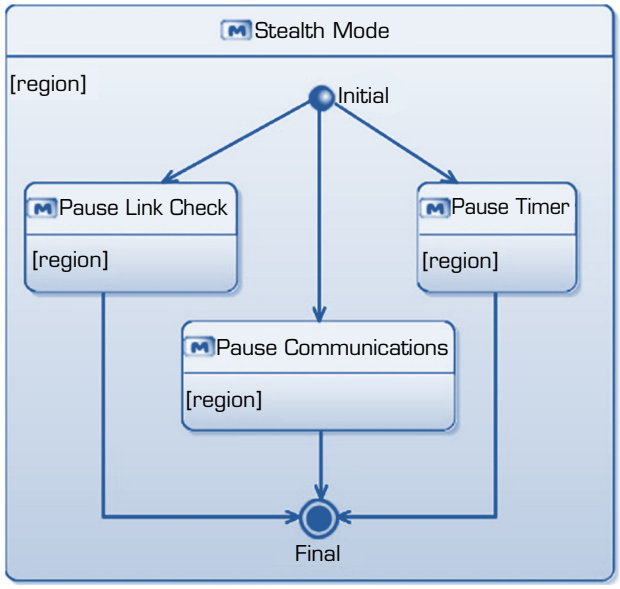
Source: Elaborated by the authors.

Figure 5. Scenarios 1 and 2: Sequence Diagram for the UA.

The UAS performs a "Check Link" function. If the link is intact, a "Link OK" signal resets the "Timer," and operations continue normally. If a "Link Failure" occurs, the Timer is not reset, and the system initiates a "Restore Link" process. If the link is restored within the timeout period, the system resumes normal operations. If not, the Timer sends a "Timed Out" signal, triggering the "Termination Decision," which may involve returning, landing, or continuing automatically, depending on predefined logic. Alternatively, a predefined number of failed restore attempts can also trigger mission termination, preventing reliance solely on the timer.

The cues that provided information about the occurrence of scenarios 1 and 2 (link degradation or loss) were identified as the intensity of the link signal, which is provided internally to the aircraft itself (that is, it can know its own link status) and to the operator (by the link monitoring provided by the GCS, and not represented in Fig 5, which focuses on the UA), so that the operator knows the link status and can make proper decisions according to the mission stage, constraints, and particularities. The critical decision point occurs when the timeout period ends, initiating the Termination Decision process.

A specific case for military UAS is "Stealth Mode," in which communications are intentionally suspended to avoid detection over hostile territory (Fig. 6). In this mode, link checks and timers are paused to prevent triggering a "Safe Mode" activation due to expected link loss. The UA continues pre-programmed tasks automatically, and the operators have no control over it to send commands. Once the conditions are met, the UAS exits Stealth Mode and becomes controllable and communicable again.



Source: Elaborated by the authors.

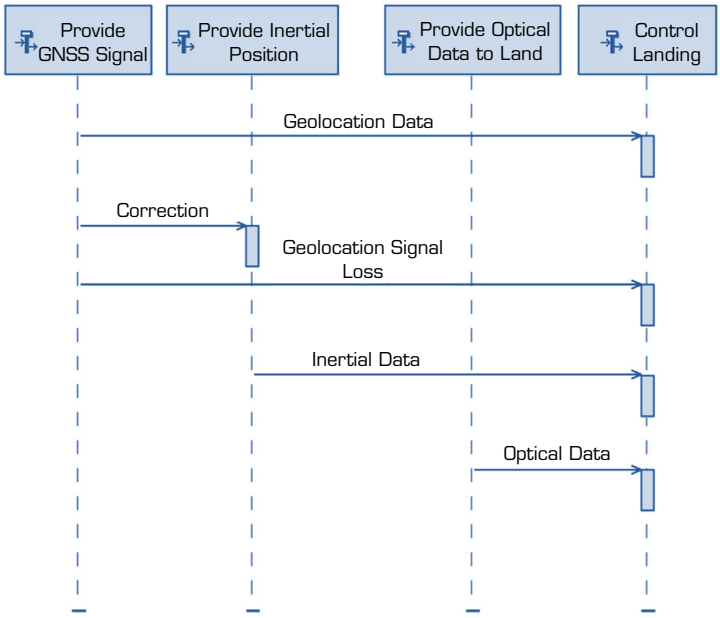
Figure 6. Stealth Mode State Machine Diagram for the UA.

Scenario 3 (GNSS signal loss)

Based on interview participants' experience, GNSS signal loss during normal operations typically leads to automatic landings, except in LOS operations, where pilots can visually guide the UA. Inertial backup systems are generally accurate enough for "Return Home" just at close range, before cumulative errors cause issues such as restricted airspace violations or loss of maneuverability in BVLOS operations.

To address the concerns of scenario 3, Fig. 7 models GNSS signal loss during landing for an aircraft equipped with inertial and optical backup systems. GNSS data serves as the primary navigation input, while the inertial system and optical sensors provide redundancy. If GNSS data is lost, the UA uses these backup systems to maintain positional awareness and complete the landing.

Relative to the cues regarding the occurrence of scenario 3, the participants interviewed indicated that some systems they operate do not display GNSS signal strength, only a loss alarm. They stated that signal intensity information could help anticipate problems and would contribute to situational awareness and operational safety.



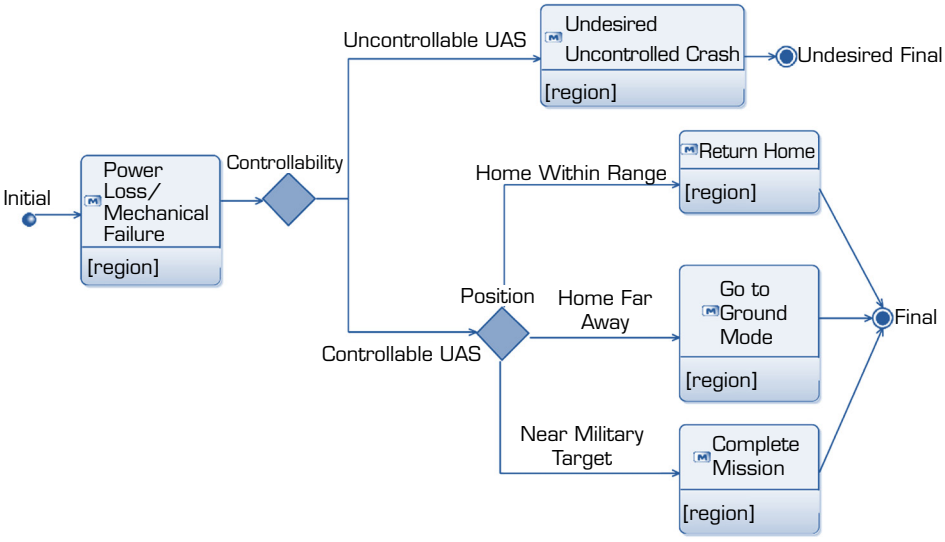
Source: Elaborated by the authors.

Figure 7. Scenario 3 Sequence Diagram for the UA.

The decision point occurs at the moment of GNSS signal loss, when the operator must choose whether to continue the mission using alternative position references (e.g., visual cues, inertial data, or Air Traffic Control [ATC] support) or to initiate a Termination Decision. In the specific case of signal loss during landing, the aircraft automatically relies on backup systems to perform the maneuver safely.

Scenarios 4 (power failure) and 5 (mechanical failure)

An integrated approach was found effective in addressing the challenges of scenarios 4 and 5, supporting flight safety under diverse conditions. A unified Sequence Diagram (Fig. 8) models system behavior based on whether the UA remains maneuverable. This distinction allows for three outcomes such as return home, complete mission or controlled landing (UA is still maneuverable), controlled crash (e.g., via parachute to reduce ground risk), and uncontrolled crash.



Source: Elaborated by the authors.

Figure 8. Scenarios 4 and 5 State Machine Diagram.

At the abstraction level targeted in this study, the primary objective is to identify the overarching characteristics and general requirements that can be applied across various system architectures. As such, multiple hypotheses and solutions are proposed for each scenario. The choice of the most appropriate hypothesis, the specific cause of an issue, and the corresponding solution for a given UA will ultimately depend on the selected architecture. Table 2 synthesizes the key cues, causes, and alternative strategies for maintaining flight safety during the occurrence of scenarios 4 and 5. However, for military UA operating in Complete Mission mode, the system will proceed to attack designated targets regardless of external conditions, rendering the considerations outlined in Table 2 inapplicable in such cases.

Table 2. Cues, possible diagnostics, and possible approaches to deal with scenarios 4 and 5.

Cue	Possible diagnostics	Continue mission	Glide (fixed-wings)	Return home	Go to ground	Observation
Aerodynamic actuators failure	Maintenance problem/ collision	X	x	x	x	Left affected aerodynamic surface "free-floating" and use the other surfaces to compensate for the torques
Low battery indication (Critical Level 1)	Low battery	X	x	x	x	The operator can choose the action
Low battery indication (Critical Level 2)	If sudden: electrical power loss/engine failure				x	Automatic UA action
Low fuel	Low fuel	X	x	x	x	The pilot can choose the action
The engine's low rotation speed	Electrical power loss/fuel leakage/fuel pump failure/ collision/engine failure		x	x	x	Return depends on the distance to home and the aircraft's height
Low engine oil pressure	Mechanical failure/oil leakage/collision/engine failure/oil pipe rupture		x	x	x	Turn the engine off
Engine oil overtemperature	Mechanical failure/ oil leakage/collision/ engine failure/cooling pipe rupture		x	x	x	Turn the engine off
Excessive vibration	Collision/engine failure				x	Turn the engine off if the vibration originates from it

Source: Elaborated by the authors.

Low battery

A two-tiered critical charge threshold can be employed to manage low battery scenarios. Upon the battery reaching "Critical Level 1," the operator is alerted and advised to initiate a Return Home command, though mission continuation is permitted briefly. If the battery reaches "Critical Level 2," the UA automatically transitions to Go to Ground Mode for an emergency landing to preserve flight safety. Sudden depletion below Critical Level 2 may result from collisions, electrical faults, or engine loss, depending on the UA's design.

One potential solution for low battery in rotary-wing UA is to harness blade rotation during descent to drive the motor as a generator, sustaining the onboard computer and enabling partial control. However, this requires motors capable of dual operation, which may not be feasible within the design constraints of the project.

If power loss disables the onboard computer, an uncontrolled crash is unavoidable. Whereas difficult to prevent across all architectures, risk can be mitigated by integrating an emergency parachute system. Enhancing safety in these scenarios increases system complexity and cost, requiring careful trade-offs among feasibility factors such as cost, size, and weight to ensure practical implementation within the overall design.

Engine power loss or low fuel level

The system architecture and wing type significantly influence the feasible responses to sudden engine power loss. For fixed-wing UAS, the appropriate action depends on altitude and distance from the base at the time of failure; the aircraft may either glide back to base or perform an emergency landing at a designated crash site. In contrast, rotary-wing UAS cannot glide. Instead, they rely on blade rotation during descent to reduce vertical speed. However, due to limited propeller inertia, these systems typically cannot achieve effective autorotation, increasing the likelihood of impact damage.

Possible causes of engine power losses may be, depending on the system architecture, electrical power loss, fuel leakage, fuel pump failure, and engine damage, and the main cues to identify these problems are battery charge indication, fuel quantity, engine rotation speed, engine oil temperature, and pressure. When the system design couples failure modes, causing an engine loss to result in a loss of power and vice versa, the aircraft's controllability and ability to mitigate damage are reduced.

In low fuel hit scenarios, the pilot shall be alerted and decide what to do, as sometimes a mission has such a priority that the pilot may decide to sacrifice the UA to complete it. Sudden leakage can be caused by a projectile hit, and the pilot may have the option to deactivate weapons in this case, to prevent accidents (such as igniting a missile near a fuel leak point). However, the pilot may decide to maintain the offensive potential of the UA in some scenarios, as mission accomplishment is sometimes more important than general safety in military operations, when risks must be taken to achieve objectives, even with losses.

Aerodynamic actuators failure

Failures in aerodynamic actuator sensors may result from mechanical damage, maintenance issues, or collisions, leading to actuator locking or loss of function. When control is lost, the ideal response is to allow the affected surface to enter a free-floating state, minimizing interference and enhancing stability. However, malfunctions may instead leave the surface locked in a fixed position.

In both cases, the onboard computer must compensate using the remaining aerodynamic surfaces to maintain control, ensuring the aircraft stays within its flight envelope and can either continue the mission, return to base, or execute an emergency landing, depending on residual controllability. Actuator locking, especially near operational extremes, poses greater challenges and requires robust, adaptive control strategies to preserve flight stability and safety. During the failure of the fixed-wing segment in hybrid VTOL UA, it can transition to a multicopter to avoid a crash.

Step 5: formulating safety requirements from scenario analysis

In Step 5, requirements were elicited for two UAS components: the UA, which comprises the airborne segment and presents potential risks to third parties, and the GCS, whose interface supports pilots in managing critical scenarios. To ensure specificity, the elicitation focused on fixed-wing military UAs with combustion engines, though most requirements are also applicable to electric UAs and rotary-wing multicopters, providing a general foundation for UAS projects. Each requirement was linked to the scenario(s) where it is most relevant, enhancing traceability. These are listed in Table 3 (UA) and Table 4 (GCS). Requirements were elicited using information about the cues, complicating factors, decision points, solutions, and preventive actions prescribed in CDM. The MBSE diagrams helped to identify interfaces of the systems (both external and relating to their internal components), in which it is necessary to alert operators about problems, and the modes of operation, for example. As previously stated, the purpose of this step is to elicit safety requirements for specific critical scenarios, to complement the general safety requirements identified by other existing techniques (which are not the focus at the moment).

Regarding the UA requirements, insights provided by experts during CDM interviews showed the critical need for autonomous flight capabilities across all scenarios (A2 and A16). In many situations, their perceptions led to solutions in which the UA automatically adjusts its control surfaces to perform actions such as returning to base, navigating to an emergency landing site, or compensating for a damaged or locked component. This approach aligns with Society of Automotive Engineers (SAE) Level 4 automation (Manage by Exception), where the system performs functions independently and only alerts the human operator in case of anomalies (JARUS 2023). The operator is not required to monitor the function continuously but can intervene when notified.

Using MBSE diagrams developed for each scenario (notably Figs. 2 and 8), the authors identified operational modes and functions linked to specific requirements. For example, Class G Mode stems from requirement A40 and imposes a climb before returning home (A41), whereas Safe Mode is defined by A31. Functions such as Return Home (A37) were also specified based on situational demands.

Table 3. Scenario-related safety requirements for the UA.

Requirement ID	Traceable to scenario(s)	Statement	Safety requirements group
A1	1, 2, 3, 4, 5	The UA shall perform an automatic pre-flight self-check with error reporting upon system initialization	General
A2	1, 2, 3, 4, 5	The UA shall operate with automation at SAE Level 4 ("Manage by Exception")	
A3	5	The UA shall operate strictly within its defined flight envelope	
A4	1, 2, 3, 4, 5	The UA shall continuously monitor electronic component health	
A5	1, 5	The UA shall continuously monitor wind speed	
A6	1, 5	The UA shall transmit wind speed data to the GCS	
A7	2, 3	The UA shall have collision avoidance sensors	
A8	1, 2, 3, 4, 5	The UA shall continuously transmit sensor data to the GCS	
A9	1, 2, 3, 4, 5	The UA shall monitor payload health	
A10	1, 2, 3, 4, 5	The UA shall transmit the health status to the GCS	
A11	4, 5	The UA shall continuously monitor structural vibrations	
A12	1, 2, 3, 4, 5	The UA shall detect potential threats	
A13	1, 2, 3, 4, 5	The UA shall detect radar targeting and laser illumination as threats	
A14	1, 2, 3, 4, 5	The UA shall communicate identified threats promptly to the GCS	
A15	1, 2, 3, 4, 5	The UA shall automatically detect inconsistencies between sensor readings and redundant sensor backups to identify sensor malfunctions early	
A16	4, 5	The UA shall incorporate adaptive flight control algorithms to handle partial aerodynamic control surface failures effectively	
A17	1, 2	The UA shall continuously monitor its communication link with the GCS	Communications
A18	1, 2	The UA shall automatically attempt to reestablish the lost communication link with the GCS	
A19	1, 2	The UA shall ensure encryption on all communication channels with the GCS	
A20	1, 2	The UA shall provide redundancy in its link with the GCS	
A21	2	The UA shall clock time since the last communication with the GCS	
A22	1, 2	The UA shall automatically prioritize critical mission data during periods of degraded communication	
A23	1, 2	The UA shall automatically detect electronic interference	
A24	1, 2	The UA shall dynamically alter communication frequencies to mitigate jamming	
A25	1, 2	The UA shall automatically notify the GCS upon detection of electronic interference	
A26	2, 3, 5	The UA shall respect the programmed restricted areas constraints	Navigation
A27	3	The UA shall transmit GNSS data to the GCS	
A28	3	The UA shall provide alternative navigation solutions to GNSS data	
A29	1, 2, 3, 4, 5	The UA shall dynamically adjust navigation paths to avoid terrain and environmental hazards	
A30	1, 2, 3	The UA shall implement a dedicated "Controlled Airspace Mode" for operations in controlled airspace	
A31	1, 2, 3, 4, 5	The UA shall implement a Safe Mode for handling emergency scenarios automatically	Safe Mode
A32	3, 4, 5	The UA shall transmit a message to ATC and to GCS informing the status when entering "Safe Mode"	
A33	1, 2, 3, 4, 5	The UA shall automatically perform pre-defined emergency procedures upon entering "Safe Mode"	
A34	1, 2, 3, 4, 5	The UA shall automatically select optimal emergency landing zones based on real-time hazard assessments	
A35	1, 2, 3, 4, 5	The UA shall implement a "Go to Ground Mode"	Go to Ground Mode
A36	1, 2, 3, 4, 5	The UA shall automatically transmit status messages to ATC and GCS upon activation of "Go to Ground Mode"	
A37	1, 2	The UA shall be able to return home automatically without pilot intervention	
A38	1, 2, 3, 4, 5	The UA shall perform autonomous controlled landings without pilot intervention	
A39	1, 2, 3, 4, 5	The UA shall deploy parachutes for emergency flight termination	
A40	1, 2	The UA shall implement Class G Mode	Class G Mode
A41	1, 2	The UA shall climb 2,000 ft before an emergency automatic Return Home in Class G Mode	

Continue...

Continuation.

A42	4, 5	The UA shall automatically activate Go to Ground Mode upon battery charge reaching Critical Level 2	Battery management
A43	4	The UA shall automatically initiate a "Battery Save Protocol" upon battery charge reaching Critical Level 2	
A44	5	The UA shall present an external connection for the battery	
A45	4, 5	The UA shall continuously monitor engine oil pressure	Engine functioning
A46	4, 5	The UA shall continuously monitor engine oil temperature	
A47	4, 5	The UA shall automatically shut down the engine in the event of a fire	
A48	4, 5	The UA shall automatically attempt an in-flight engine restart after an uncommanded shutdown	
A49	4, 5	The UA shall continuously monitor the fuel level	
A50	1, 2, 3, 4, 5	The UA shall implement a Complete Mission Mode	Complete Mission Mode
A51	1, 2, 3, 4, 5	The UA shall automatically search the target in Complete Mission Mode	
A52	1, 2, 3, 4, 5	The UA shall automatically track the target in Complete Mission Mode	
A53	1, 2, 3, 4, 5	The UA shall automatically engage the target in Complete Mission Mode	
A54	1, 2, 3, 4, 5	The UA shall automatically evade the area after engaging the target in Complete Mission Mode	
A55	1, 2, 3, 4, 5	The UA shall prioritize Complete Mission Mode when activated over any other functions	
A56	2	The UA shall implement a Stealth Mode	Stealth Mode
A57	2	The UA shall pause link check in Stealth Mode	
A58	2	The UA shall pause communications in Stealth Mode	
A59	2	The UA shall accept input conditions to start and exit Stealth Mode	
A60	2	The UA shall automatically exit Stealth Mode when conditions are reached	
A61	2	The UA shall allow keeping Complete Mission Mode and Stealth Mode enabled at the same time	
A62	5	The UA shall present deactivatable anti-collision lights	
A63	5	The UA shall inhibit weapons when on the ground (weight-on-wheels)	Weapons safety
A64	4, 5	The UA shall allow individual weapons deactivation by the pilot	
A65	4, 5	The UA shall allow individual weapons emergency disposal (droppage)	
A66	4, 5	The UA shall automatically deactivate each weapon before disposing it	
A67	4	The UA shall automatically deactivate weapons upon reaching Critical Level 2 battery level	
A68	4, 5	The UA shall automatically deactivate weapons in Safe Mode	

Source: Elaborated by the authors.

Table 4. Scenario-related safety requirements for the Ground Control Station.

Requirement ID	Traceable to scenario(s)	Statement	Safety requirements group
G1	1, 2, 3, 4, 5	The GCS shall display the error log generated upon UA initialization	General
G2	1, 2, 3, 4, 5	The GCS shall display real-time UA status information	
G3	1, 2, 3, 4, 5	The GCS shall automatically log flight data, system status changes, faults, sensor anomalies, and alerts for post-mission analysis	
G4	4, 5	The GCS shall apply predictive analytics to historical operational data and maintenance records to anticipate UA system malfunctions	
G5	4, 5	The GCS shall automatically alert the operator about recommended preventive maintenance actions	
G6	1, 2, 3, 4, 5	The GCS shall provide quick-command shortcuts for frequently used operations	
G7	1, 5	The GCS shall display real-time UA wind speed	
G8	5	The GCS shall allow visual indication of safe boundaries of the UA flight envelope in real-time	
G9	5	The GCS shall automatically restrict pilot commands that exceed defined safe operational parameters	
G10	3	The GCS shall display images from the UA's optical sensors	
G11	3	The GCS shall display UA GNSS data	
G12	4, 5	The GCS shall display the UA engine oil pressure	
G13	4, 5	The GCS shall display the UA engine oil temperature	
G14	4, 5	The GCS shall display the UA fuel level	
G15	1, 2, 3, 4, 5	The GCS shall display the UA health status	
G16	1, 2, 3, 4, 5	The GCS shall provide decision-support tools for operators during complex or ambiguous scenarios	

Continue...

Continuation.

G17	1, 2	The GCS shall continuously monitor the communication link strength with the UA	Communications
G18	1, 2	The GCS shall display the communication link strength with the UA	
G19	1, 2	The GCS shall support redundant communication links with the UA	
G20	1, 2	The GCS shall utilize encrypted communication channels with the UA	
G21	1, 2, 3, 4, 5	The GCS shall support rapid transmission of critical UA status updates to ATC using standardized protocols	
G22	3	The GCS shall display real-time GNSS signal strength from the UA	Navigation
G23	2, 3, 5	The GCS shall allow saving the programmed restricted area constraints	
G24	1, 3, 4, 5	The GCS shall display a map of the flight region with boundaries and constraints (aerodromes, no-fly zones, threats, etc.).	
G25	1, 3, 4, 5	The GCS shall allow manual edits to pre-programmed flight routes	
G26	1, 3, 4, 5	The GCS shall display pre-programmed route options	
G27	1, 2, 3, 4, 5	The GCS shall display alternative pre-planned routes	
G28	1, 3, 4, 5	The GCS shall allow uploading previously saved flight plans	
G29	5	The GCS shall allow displaying the future trajectory of the UA, considering UA speed and altitude	
G30	1, 2, 3, 4, 5	The GCS shall support pilot-confirmed rerouting to alternative landing sites in response to critical UA status alerts	
G31	1, 2	The GCS shall require operator confirmation for validation of waypoints located in no-fly zones	
G32	4	The GCS shall continuously estimate remaining operational flight time based on real-time conditions (fuel, battery, environment)	
G33	4, 5	The GCS shall display other airspace users and hazards identified through cooperative surveillance systems	
G34	1, 2, 5	The GCS shall present meteorological conditions using a color-coded hazard heat-map	
G35	1, 2, 3, 4, 5	The UA shall present a command to activate Return Home Mode	Safe Mode
G36	1, 2, 3, 4, 5	The GCS shall automatically notify ATC upon activation of UA Safe Mode	
G37	4	The GCS shall activate an alert when the UA battery charge reaches Critical Level 1	Battery management
G38	4	The GCS shall display the option Return Home when the UA battery charge reaches Critical Level 1	
G39	4	The GCS shall display the option to activate Safe Mode when the UA battery charge reaches Critical Level 1	
G40	4, 5	The GCS shall allow the pilot to issue weapons commands (fire, deactivate weapons, and drop weapons)	Weapons
G41	1, 2, 3, 4, 5	The GCS shall clearly differentiate alarms and alerts by severity level (critical, warning, informational) using distinct audible tones and visual indications	Flight alerts
G42	1, 2, 3, 4, 5	The GCS shall automatically correlate multiple alerts into consolidated notifications to prevent operator overload	
G43	1, 2, 3, 4, 5	The GCS shall display an alert when Safe Mode is activated	
G44	5	The GCS shall alert the pilot if the UA approaches unsafe conditions	
G45	1, 2, 3	The GCS shall display spoofing detection alerts	
G46	1, 2, 3	The GCS shall display jamming detection alerts	
G47	1, 2, 3, 4, 5	The GCS shall activate alerts upon detecting potential operational threats	
G48	1, 2, 3, 4, 5	The GCS shall display potential threats on the map	
G49	1, 2, 4, 5	The GCS shall activate an alert upon loss of the communication link with the UA	
G50	3	The GCS shall activate an alert upon loss of GNSS signal from the UA	
G51	1, 2, 3, 4, 5	The GCS shall provide a simulation mode for operator training on handling identified critical scenarios	Training

Source: Elaborated by the authors.

Interviews with maintainers and operators identified key cues indicating engine problems, such as excessive vibration (A11), high oil temperature (A46), or low pressure (A45), along with typical response strategies. Based on these insights, the UA could automatically shut down the engine in case of fire (A47) and attempt in-flight restarts after failure (A48), while preserving the pilot's authority to override and take control.

The MBSE Sequence Diagram for the GNSS signal loss scenario (Fig. 7) supported the elicitation of requirements for fallback strategies, such as obstacle avoidance (A29) and safe landing using backup systems (A38), and the use of parachutes for flight

termination can enhance safety (A39). The inclusion of deactivable anti-collision lights (A62) ensures compliance with the legal regulations while maintaining compatibility with stealth operations, which are considered in requirements from A56 to A62, identified from the diagram in Fig. 6.

The military requirements to complete the mission even under interference or after being hit by air defenses, as elicited from Fig. 4, are addressed in requirements A50 to A55, prioritizing the "Complete Mission Mode" over other functions to prevent external interference from triggering an unintended Safe Mode that could compromise target engagement.

The safety requirements related to weapons aim to prevent accidental discharges on the ground or during pre-flight procedures (A63) and to ensure the deactivation of weapons that must be jettisoned in emergencies or due to launch failures (A66), minimizing the risk of harm to people on the ground.

Regarding the GCS, the system shall notify the operator and require explicit confirmation before authorizing the insertion of a waypoint in a restricted area (G31), ensuring that such operations occur only when strictly necessary for the mission.

The UA shall monitor wind speed (A5), and the GCS shall display this data to the pilot (G7), enabling the definition of safe flight boundaries (G8). Wind speed is critical for assessing proximity to the flight envelope limits, which the UA shall automatically maintain (A3). The GCS shall also restrict improper pilot inputs (G9) to prevent loss of control. Similarly, continuous monitoring of system health, link signal strength, GNSS signal, and presenting this information to the operator (A9, G15, G17, G18, G11), is essential for situational awareness in emerging critical scenarios and to ensure compliance with SORA OSO #19/#20 low robustness airworthiness requirements (EASA 2024).

Battery status must be monitored, with visual and/or audible alerts provided to the pilot (G37). These alerts are particularly important for flight planning and for informing both the pilot and ATC in case the UA activates Safe Mode (G36). Operators emphasized that these features are especially helpful during high-stress missions, when situational awareness and human performance may degrade.

Automatic predictive maintenance tasks using flight and maintenance data (G1, G3, G4, G5) were also considered essential by experts. This reduces the likelihood of scenarios 4 and 5 (electrical or mechanical failure) by anticipating component degradation (e.g., end-of-life batteries, actuators with abnormal vibrations).

Coordination with ATC is important throughout all flight phases. The CDM interviews revealed that ATC input can be key to understanding critical events in BVLOS operations. For instance, communication alone may be ambiguous. However, if ATC reports that the UA maintains or gains altitude, it may indicate scenario 2 (communication loss). A sudden altitude drop, conversely, may point to scenario 4 (power failure), with communication loss as a consequence. This underscores the importance of integrating external information sources (G33) to enhance situational awareness and mitigate risks.

The analysis of the MBSE Sequence Diagram for the communication loss scenario (Fig. 5) supported the elicitation of requirements for link monitoring (A17) and automatic reestablishment attempts (A18).

Military UAs may also include automatic threat detection systems (A12, A13), as evidenced in MBSE diagrams that map mission threats and targets. The GCS shall alert pilots to electronic interference events, such as spoofing or jamming (G45, G46), and to detected threats (G47), supporting mission safety and effectiveness.

Excessive information on the GCS display can reduce operational safety (G41). Replacing non-critical data with warning messages or automating responses when appropriate is recommended. For example, in the case of abnormal engine oil pressure or temperature, automation may be preferable to continuous monitoring. As stated in SORA OSO #19/#20, if only one suitable response exists (e.g., automated landing), presenting detailed information may be counterproductive, and automation should take precedence.

Comparison of the results with UAS certification standards, safety regulations, and alignment with current themes

The EASA and FAA regulations specify general requirements that UAS manufacturers must comply with, as well as the type of evidence required for certification. However, these standards have a more general character, are not focused on specific operational scenarios, and are not sufficient to develop UAS, but rather constitute the minimum requirements and guidance for authorities to certify them. The proposed CDM-based method complements regulatory frameworks, such as JARUS SORA and FAA Part

107, by providing a structured approach to identify and elicit scenario-specific safety requirements. Whereas JARUS SORA offers broad guidance on demonstrating operational safety, the CDM method described here systematically translates critical operational insights into actionable design requirements.

In alignment with MIL-STD-882E, which structures hazard identification and risk mitigation through preliminary hazard analysis (PHA) and system safety assessments (SSA) (Department of Defense 2012), the CDM stage supports the qualitative identification of hazard sources and operational decision points derived from expert experience. Similarly, ARP4761A (SAE International Recommended Practice 2023) emphasizes functional hazard assessment (FHA) and the definition of development assurance levels (DAL) through analytical techniques such as preliminary system safety assessment (PSSA), fault tree analysis (FTA), and failure modes and effects analysis (FMEA). The MBSE integration proposed in this paper provides a formal mechanism to map these hazards to model elements and system requirements early in the design phase and supports current advances in human–autonomy teaming (HAT) by formalizing expert decision logic that can be embedded in autonomous behaviors, enhancing transparency and trust. From a resilience engineering perspective, the framework strengthens system adaptability by translating human coping strategies into model-based requirements that anticipate degraded or unexpected states. Furthermore, coupling CDM-derived decision models with artificial intelligence (AI)-assisted decision-support systems could enable continuous verification of safety behaviors and facilitate explainable autonomy, in which each automated action remains traceable to human-elicited rationale.

Finally, consistent with ISO/IEC/IEEE 15288, the method enriches the requirements definition process, serving as a practical extension of existing regulatory requirements, by enhancing the traceability, relevance, and applicability of safety measures. These connections position the proposed methodology within ongoing international research efforts toward intelligent, certifiable, and resilient safety-critical systems. The case study illustrates its practical application to a military UAS, offering a replicable foundation for similar projects.

CONCLUSION

This study presented a structured methodology integrating CDM and MBSE to systematically elicit safety requirements for UAS in critical scenarios, which was effective in identifying a total of 119 requirements, comprising 68 for the UA and 51 for the GCS.

The CDM framework proved effective in guiding interviews with stakeholders who possess direct experience with UAS and are familiar with the operational conditions that can compromise safety performance. However, due to the time-intensive nature of conducting and analyzing these interviews, careful selection of critical scenarios is essential to maintain feasibility.

In terms of participant selection, the inclusion of stakeholders from multiple domains (operators, certifiers, designers, and maintainers) ensured broader coverage of safety challenges encountered across different phases of UAS operation. This multidisciplinary approach helped capture a diverse range of risks and mitigation strategies, contributing to a more comprehensive requirement set, complementing existing regulations and standards requirements, and aligning with industry practices.

Complementarily, MBSE facilitated the organization, visualization, and integration of these insights into coherent and traceable requirements. Diagrams such as Sequence Diagrams, State Machine Diagrams, and Use Case Diagrams significantly improved the clarity and understanding of system behaviors, enabling effective validation and communication among stakeholders.

Beyond the method itself, another key contribution of this study lies in the results it generated: the insights obtained from expert interviews and the set of safety requirements identified in the case study. These findings are not only relevant to the specific UAS project analyzed but can also serve as a valuable resource for other teams developing UAS, helping to enhance their design processes and improve operational safety. The requirements and insights can guide safety considerations, risk mitigation strategies, and best practices, making them applicable to a wide range of UAS platforms. By making these findings available, this study contributes to the broader effort to improve UAS safety, supporting more robust and well-informed development processes.

CONFLICTS OF INTEREST

Nothing to declare.

AUTHOR CONTRIBUTIONS

Conceptualization: Casale DE; **Methodology:** Casale DE; **Formal analysis:** Casale DE; **Investigation:** Casale DE, Silva RC, and Viana Júnior JTL; **Writing - Original Draft:** Casale DE; **Writing - Review & Editing:** Casale DE, Silva RC, Viana Júnior JTL, and Cardoso Junior MM; **Visualization:** Casale DE and Silva RC; **Supervision:** Casale DE, Cardoso Junior MM, and Costa LEVL; **Project administration:** Casale DE; **Funding acquisition:** Casale DE, Cardoso Junior MM, and Costa LEVL; **Final approval:** Casale DE.

DATA AVAILABILITY STATEMENT

All data sets were generated or analyzed in the current study.

FUNDING

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil
Finance Code 001.

DECLARATION OF USE OF ARTIFICIAL INTELLIGENCE TOOLS

In the preparation of this manuscript, AI tools were utilized to support language refinement. Gemini (Google) was employed for grammatical correction and proofreading. No AI tool was involved in the conceptualization, methodology, data analysis, or interpretation of results.

ACKNOWLEDGEMENTS

We acknowledge to CAPES, as this study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. The authors gratefully acknowledge the Brazilian Army Aviation (Aviação do Exército) and the Brazilian Air Force (Força Aérea Brasileira) for making their technical personnel available to support this research.

REFERENCES

[EASA] European Union Aviation Safety Agency (2024) Proposed CM–HF-001 issue 01 – safe recovery from human errors and HMI appropriate for the mission (SORA OSO#19/#20 low robustness airworthiness requirements). https://www.easa.europa.eu/en/document-library/product-certification-consultations/proposed-cm-hf-001-issue-01-safe-recovery

[INCOSE] International Council on Systems Engineering (2021) Systems engineering vision 2035. https://sevisionweb.incose.org/?utm_source=chatgpt.com

[JARUS] Joint Authorities for Rulemaking on Unmanned Systems (2024) Guidelines on specific operations risk assessment (SORA). Pub No. JAR-DEL-SRM-SORA-MB-2.5. http://jarus-rpas.org/wp-content/uploads/2024/06/SORA-v2.5-Main-Body-Release-JAR_doc_25.pdf

[JARUS] Joint Authorities for Rulemaking on Unmanned Systems (2023) Methodology for evaluation of automation for UAS operations. Pub No. JARUS-Doc-AutoMethod.1.0. http://jarus-rpas.org/wp-content/uploads/2023/06/jar_21_doc_JARUS_Methodology_for_Evaluation_of_Automation_for_UAS_Operations.pdf

[SAE] Society of Automotive Engineers (2023) Guidelines for conducting the safety assessment process on civil aircraft, systems, and equipment. SAE International Recommended Practice ARP4761A. https://doi.org/10.4271/ARP4761A

Akram F, Ahmad T, Sadiq Mohd (2024) Recommendation systems-based software requirements elicitation process – A systematic literature review. J Eng Appl Sci 71(1):29. https://doi.org/10.1186/s44147-024-00363-4

Asmayawati S, Nixon J (2020) Modelling and supporting flight crew decision-making during aircraft engine malfunctions: developing design recommendations from cognitive work analysis. Appl Ergon 82:102953. https://doi.org/10.1016/j.apergo.2019.102953

Avelino B, Caetano M, Silva EJ (2023) Um modelo conceitual para drones e caminhões cooperativos inteligentes em operação logística. Aplic Oper Em Áreas Def 24(1):24-28. https://doi.org/10.55972/spectrum.v24i1.390

Carson RS (2015) Implementing structured requirements to improve requirements quality. INCOSE Int Symp 25(1). https://doi.org/10.1002/j.2334-5837.2015.00048.x

Casale DE, Silva RC, Cardoso Júnior MM, Costa LEVL (2025) Abordagem multicritério para seleção de conceito de veículo aéreo não tripulado (VANT) de combate. Revista da Escola de Guerra Naval 31(1). https://doi.org/10.21544/2359-3075.31125

Cattermole VT, Horberry T, Hassall M (2016) Using naturalistic decision making to identify support requirements in the traffic incident management work environment. J Cogn Eng Decis Mak 10(3):309-324. https://doi.org/10.1177/1555343416655509

Dar H, Lali MI, Ashraf H, Ramzan M, Amjad T, Shahzad B (2018) A systematic study on software requirements elicitation techniques and its challenges in mobile application development. IEEE Access 6:63859-63867. https://doi.org/10.1109/ACCESS.2018.2874981

De Carvalho Lourenço C, Cardoso Júnior MM (2025) Naturalistic decision-making in military aviation: significant milestones, trends and gaps. Paper presented 2025 22nd Congress of the International Ergonomics Association. IEA; Singapore. https://doi.org/10.1007/978-981-96-9334-4_7

Department of Defense (2012) Department of Defense standard practice: system safety. https://www.nde-ed.org/NDEEngineering/SafeDesign/MIL-STD-882E.pdf

Dick J, Hull E, Jackson K (2017) Requirements engineering. Cham: Springer. https://doi.org/10.1007/978-3-319-61073-3

Douglass BP (2016) Agile systems engineering. Waltham: Morgan Kaufmann. https://doi.org/10.1016/C2014-0-02102-8

Du S, Zhong G, Wang F, Pang B, Zhang H, Jiao Q (2024) Safety risk modelling and assessment of civil unmanned aircraft system operations: a comprehensive review. Drones 8(8):354. https://doi.org/10.3390/drones8080354

Friedenthal S, Griego R, Sampson M (2007) INCOSE model based systems engineering (MBSE) initiative. https://www.researchgate.net/profile/Mark-Sampson/publication/267687693_INCOSE_Model_Based_Systems_Engineering_MBSE_Initiative/links/54ca7c290cf22f98631b167e/INCOSE-Model-Based-Systems-Engineering-MBSE-Initiative.pdf

Grindley B, Phillips K, Parnell KJ, Cherrett T, Scanlan J, Plant KL (2024) Over a decade of UAV incidents: a human factors analysis of causal factors. Appl Ergon 121:104355. https://doi.org/10.1016/j.apergo.2024.104355

Gupta A, Afrin T, Scully E, Yodo N (2021) Advances of UAVs toward future transportation: the state-of-the-art, challenges, and opportunities. Future Transp 1(2):326-350. https://doi.org/10.3390/futuretransp1020019

Hart S, Banks V, Bullock S, Noyes J (2022) Understanding human decision-making when controlling UAVs in a search and rescue application. AHFE Open Access 68. https://doi.org/10.54941/ahfe1002768

Hoebbel CL, Bellanca JL, Hrica JK (2024) Lessons learned from haul truck operator near-miss events: use of the critical decision method to identify strategies to improve operator safety in mining. Min Metall Explor 41. https://doi.org/10.1007/s42461-024-01066-3

Iqbal D, Abbas A, Ali M, Khan MUS, Nawaz R (2020) Requirement validation for embedded systems in automotive industry through modeling. IEEE Access 8:8697-8719. https://doi.org/10.1109/ACCESS.2019.2963774

ISO/IEC/IEEE (2023) Systems and software engineering – System life cycle processes. ISO/IEC/IEEE 15288:2023. https://doi.org/10.1109/IEEESTD.2023.10123367

Kahan E, Genero M, Oliveros A (2024) Refining a design thinking-based requirements elicitation process: insights from a focus group. Sci Comput Program 237:103137. https://doi.org/10.1016/j.scico.2024.103137

Karakhan AA, Al-Mhdawi MKS (2024) Risks associated with using drones in construction for safety management. Pract Period Struct Des Constr 29(4). https://doi.org/10.1061/PPSCFX.SCENG-1543

Klein GA, Calderwood R, Macgregor D (1989) Critical decision method for eliciting knowledge. IEEE Trans Syst Man Cybern 19(3). https://doi.org/10.1109/21.31053

Klinger DW, Gomes ME (1993) A cognitive systems engineering application for interface design. Proceedings of the Human Factors and Ergonomics Society Annual Meetingt 37(1):16-20. https://doi.org/10.1177/154193129303700105

Larson W, Kirkpatrick D, Sellers J, Thomas L, Verma D (2009) Applied space systems engineering. New York: McGraw-Hill.

Mansikka H, Virtanen K, Lipponen T, Harris D (2024) Improving pilots' tactical decisions in air combat training using the critical decision method. Aeronaut J 128(1326):1613-1626. https://doi.org/10.1017/aer.2024.3

Mendes WS (2018) Um método de modelagem descritiva de sistemas de engenharia para possibilitar a geração automática de requisitos textuais aplicado a um satélite (PhD thesis). São José dos Campos: Instituto Nacional de Pesquisas Espaciais. In Portugues. http://urlib.net/sid.inpe.br/mtc-m21b/2018/01.08.19.24

Plant KL, Stanton NA (2016) Distributed cognition and reality: how pilots and crews make decisions. Boca Raton: CRC Press. https://doi.org/10.1201/9781315577647

Reiser C, Villani E, Cardoso Júnior MM (2024) A novel approach to runway overrun risk assessment using FRAM and flight data monitoring. Aeronaut J 128(1327):2054-2072. https://doi.org/10.1017/aer.2024.37

Rodrigues RG, Fulindi JB, Oliveira DBP, Moraes AO, Marini-Pereira L (2022) Safety analysis of GNSS parallel runway approach operation at Guarulhos International Airport. J Aerosp Technol Manag 14. https://doi.org/10.1590/jatm.v14.1260

Russo AC, Cardoso Junior MM, Villani E (2025) Eye-tracking analysis to assess the mental load of unmanned aerial system operators: systematic review and future directions. Aeronaut J 129(1333):529-558. https://doi.org/10.1017/aer.2024.122

Saxena VR, Yadav R, Parveen A, Sadiq Mohd (2024) A mathematical model for the selection of software requirements elicitation techniques. Paper presented 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence). Amity University Uttar Pradesh; Noida, India. https://doi.org/10.1109/Confluence60223.2024.10463258

Subahi AF (2023) BERT-based approach for greening software requirements engineering through non-functional requirements. IEEE Access 11:103001-103013. https://doi.org/10.1109/ACCESS.2023.3317798

Tostes ASM, Marini-Pereira L, Moraes AO, Peixoto L, Dietzsch G, Smidt CS, Lacerda MG, Habermann M (2025) Feasibility assessment of unmanned aerial systems for precision approach path indicator inspections: a cost-effective and sustainable alternative. J Aerosp Technol Manag 17. https://doi.org/10.1590/jatm.v17.1384