Joint Authorities for Rulemaking of Unmanned Systems

# Joint Authorities for Rulemaking of Unmanned Systems

# JARUS Methodology for Evaluation of Automation for UAS Operations

**DOCUMENT IDENTIFIER : JARUS-Doc-AutoMethod.1.0**

| | | |
|---|---|---|
| **Edition Number** | : | **1.0** |
| **Edition Date** | : | **April 21, 2023** |
| **Status** | : | **Published** |
| **Intended for** | : | **General Public** |
| **Category** | : | **Publication** |
| **WG** | : | **Automation** |

# DOCUMENT CHARACTERISTICS

## TITLE

# JARUS Methodology for Evaluation of Automation for UAS Operations

| | | |
|---|---|---|
| | **Publications Reference:** | JAR-doc-AutoMethod |
| | **ID Number:** | TBD |
| **Document Identifier** | **Edition Number:** | 1.0 |
| **JARUS-Doc-AutoMethod.1.0** | **Edition Date:** | **21 April 2023** |

**Abstract**

This document is intended to provide a standard view on how to assess functional automation for the JARUS community.

The JARUS Automation WG has been tasked with defining a framework for assessing the impact of automation on an concept of operations and developing a framework for evaluating automation in proposed UAS operations. The framework includes definitions, assumptions, levels of automation, and the safety impact assessment methodology.

The roles of the manufacturer, operator, pilot, service providers, and regulators are also assessed for each level of automation.

**Keywords**

Autonomy,
Automation,
ConOps,
Trusted Autonomy

| Contact Person(s) | Tel | Unit |
|---|---|---|
| Automation WG | | TBD |

## STATUS, AUDIENCE, AND ACCESSIBILITY

| Status | | Intended for | | Accessible via | |
|---|---|---|---|---|---|
| Working Draft | ☐ | General Public | ☑ | Intranet | ☐ |
| Draft | ☐ | JARUS members | ☐ | Extranet | ☐ |
| Proposed Issue | ☑ | Restricted | ☐ | Internet (http://jarus-rpas.org) | ☑ |
| Released Issue | ☐ | Internal/External consultation | ☐ | | |

# DOCUMENT APPROVAL

The following table identifies the process of successively approving the present issue of this document before public publication.

| PROCESS | NAME AND SIGNATURE WG leader | DATE |
|---|---|---|
| WG | Craig Bloch-Hansen | August 5, 2021 |
| Internal Consultation | Craig Bloch-Hansen | January 13, 2023 |
| External Consultation | Craig Bloch-Hansen | April 21, 2023 |
|  |  |  |
|  |  |  |
|  |  |  |

## Working Group Participants

| | | |
|---|---|---|
| Craig Bloch-Hansen | Santiago Llucia | Alex Gardi |
| Costantino Senatore | Tim Kazik | Ruby Sayyed |
| Roberto Gandara Ossel | Wes Ryan | David Martin Gomez |
| Michael Shedden | Parimal Kopardekar | Christopher Eisele |
| Andrew Berry | Alberto Gaspar Martin | Carlos Cirilo |
| Xiang Zou | Angelica Cristina Robles Quilca | Akaki Kunchalia |
| Tristan Maitre | Keith Mahelo | Todd Donovan |
| Marco Ducci | Renli Lyu | Eugenio Diotalevi |
| Alan (Stan) Parkinson | Marc Baumgartner | Daniel Jost |
| Chris Swider | Bensen Koh | Kenneth Chircop |
| Marcus Johnson | Andrew Thurling | Sergio Velotto |
| Ennio Borgna | Gabrielle Wain | Diego Ernesto Zaglul González |
| Praveen Raju | Jose Martin | Scott Blum |
| Noureddin Ghazavi | Tyson Toews | |
| Andreaa Perca | Roberto Sabatini | |

# DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

| EDITION NUMBER | EDITION DATE | REASON FOR CHANGE | PAGES AFFECTED |
|---|---|---|---|
| 1.0 | 21 Apr 2023 | Initial Publication | All |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**JARUS**
**Author's name: Automation WG**
E-mail: Secretariat@jarus-rpas.org

# CONTENTS

# LIST OF FIGURES

# EXECUTIVE SUMMARY

This document proposes a classification and impact analysis scheme to help support discussions and regulatory development for automated UAS operations centred on the role of the human in performing operational functions. It also introduces the Operational Design Domain (ODD) concept as a mechanism to scope automated functions to help manage a complex multi-dimensional operational environment. This allows for a functional evaluation of automation as it relates to the human-machine interactions, recognizing that, in a particular operation, different aircraft functions may be automated to different levels.

At present the scope of the document has been limited to UAS Flight Operations while acknowledging that the flight operations will be conducted within the broader scope of the airspace environment. The automation of the airspace environment will be addressed by a future JARUS document. The document also discusses how responsibility and authority change as increasing levels of automation are introduced. The classification approach proposed builds off similar work conducted by other aviation groups including the widely publicized SAE International classification for the automotive sector and ASTM International considerations for aircraft automation (see References below). The approach to classification is summarized as follows:

> **Level 0 – Manual Operation**: The human fully responsible for function execution, with no machine support.
>
> **Level 1 – Assisted Operation**: The machine operates in an out-of-the-loop supporting role to the human in executing the function, e.g., provision of relevant information.
>
> **Level 2 – Task Reduction**: The machine operates in an in-the-loop management role in reducing human workload to accomplish the task, e.g., conflict alert and resolution advisory based on predicted flight paths.
>
> **Level 3 – Supervised Automation**: The machine executes the function under the supervision of the human who is expected to monitor and intervene as required, e.g., an automatic traffic collision and avoidance (TCAS) system tied to an autopilot which can automatically perform a manoeuvre when a Resolution Advisory is alerted.
>
> **Level 4 – Manage by Exception**: The machine executes the function alerting the human in the event of an issue. The human is not required to monitor the function in real time and is able to intervene at any time after being alerted by the machine to an issue.
>
> **Level 5 – Full Automation**: The machine is fully responsible for function execution. The human is unable to intervene in real-time either due to practical limitations or deliberate exclusion within the ODD.

The impact of the automated functions on the operation is categorized into three general levels: safety independent functions, partially safety dependent functions, and safety dependent functions. By evaluating the safety criticality of an automated function (through understanding its independence from other systems) and understanding the level to which the function is automated, the impact of automated functions on a particular operation can be assessed.

Finally, in order to fully adopt automated functions across the airspace, trust in the automated systems needs to be built. The application of trust frameworks in the development of autonomous technologies and the training of human operators is a core aspect to achieving fully autonomous system operations. In an operational environment this creates a two-way relationship between the automated machines and their human operators in order to ensure the safest application of automated operations as trusted autonomy.

# INTRODUCTION

Automation is largely implemented and understood by the community in aviation and more widely within all modern industries. However, the word autonomy is more and more used when discussing UAS operations, and a lot of misunderstanding has arisen from using this terminology.

This document aims to provide a common framework within JARUS to have productive discussions around the implementation and impact of progressive automation of functions. This document describes terms not with the aim of advocating for the approval of specific operations or systems, but rather to provide a consistent context for regulators, industry, and standardization. It is recognized that technologies, operational procedures, and infrastructure deployment may not be mature enough at this point in time to realize every concept described in this document.

# 1. Background

## 1.1 Purpose of the document

This document discusses automation and autonomy to achieve a sufficient level of shared understanding of these two concepts among the JARUS members. In addition, the document seeks to set out a common framework and design/approval considerations for JARUS to consider in the development of detailed deliverables associated with automation and autonomy.

## 1.2 Scope of the document

This document solely discusses automation and autonomy at a high level. While there are concepts described in this document that borrow from traditional aviation approaches (e.g., system safety) the intention is to provide a simplified approach to describing the effects of automation (traditional approaches are referenced throughout the document as examples of how this assessment might be expanded on in more detail for a particular operational implementation). The details are intended to be developed in subsequent JARUS documents. Examples are used in this document to illustrate concepts while providing context for the text; they may not always be applicable to all operations, or regulatory contexts.

This document provides a methodology to assess automation as part of a particular concept of operation. A second JARUS document is being developed to address airspace design and air traffic systems, including systems integration.

1) UAS Flight Operations – Refers to the portion of the UAS operation which is related to the direct control of the UA during each phase of flight including responding to adverse/degraded operating conditions which may exist during flight (note: this scope is dependent on the particular operation and may include multiple UAs and control stations as well as different airspace and air traffic control environments).
2) System Interactions – Refers to the systems which support flight operations and includes, but is not limited to, maintenance systems and air traffic management systems. While Flight Operations may be part of a larger system, and may have self-contained systems itself, for conceptual purposes the terms are considered independently.

## 1.3 Applicability

This document is intended to be used in support of JARUS deliverable development but may be useful in other contexts such as guidance to regulators looking to develop regulatory practices around automation. It may also support current and future industry efforts around automation (e.g., standards development organizations).

## 1.4 Definitions

Numerous definitions of automation and automatic system functions have been defined and redefined by various transportation technology groups over the years, including SAE, ASTM, NASA, and ICAO. To avoid confusion or conflation of terms the following terms are defined within the scope of this document:

Automation: The use of machines or computers instead of people to perform a task (Adapted from ASTM TR-1 EB).

Autonomous System(s): Have the ability and authority of decision making, problem-solving, and/or self-governance under possibly bounded, variable, or abnormal conditions (Deterministic or Non-deterministic; Adapted from National Research Council of Canada).

Degraded Mode: Refers to a system that has lost a functional capability, but may continue to operate safely under defined limitations.

Human-in-the-Loop: A system control method where a human directly provides inputs and evaluates outputs to manage system parameters (Adapted from ASTM TR-1 EB).

Human-on-the-Loop: A method of system control in which a human monitors a machine that provides inputs and evaluates outputs to manage system parameters. The human may take over the control at any point (come into-the-loop) (Adapted from ASTM TR-1 EB).

Human-off-the-Loop: A method of system control in which no human is monitoring the system control. A machine provides inputs and evaluates outputs to manage system parameters (Adapted from ASTM TR-1 EB "Human-out-of-the-Loop").

Human-Machine Symbiosis: The highest level of integration that can be achieved between the human and the system with the goal of seamlessly sharing airspace & operational information and intention (adapted from Symbiotic Systems Whitepaper).

Operational Design Domains (ODD): Operating conditions and limitations under which a given autonomous system or feature thereof is specifically designed to function, including environmental, geographical, time-of-day restrictions, and/or the requisite presence or absence of specific operational characteristics (Adapted from SAE J3016). When defining an ODD the function of the feature or system in normal, contingency, and emergency operations should be considered along with assumptions around the acceptable inputs and outputs for that function.

Object and Event Detection and Response OEDR: The subtasks of the dynamic flight task that include monitoring the flying environment (detecting, recognizing, and classifying objects and events and preparing to respond as needed) and executing an appropriate response to such objects and events. (Adapted from SAE J3016)

Phase of Flight: For this document, phase of flight refers to a period within a flight including ground operations. In the case of a human-occupied aircraft, a flight begins when any person boards the aircraft with the intention of flight and continues until all such persons have disembarked. In the case of an unoccupied aircraft, a flight begins when the aircraft is ready to move with the purpose of flight and continues until it comes to rest at the end of the flight and the primary propulsion system is shut down. (From CAST Common Taxonomy);

Robust: Robustness is achieved using both the level of integrity (i.e., safety gain) provided by each mitigation, and the level of assurance (i.e., method of proof) that the claimed safety gain has been achieved (from JARUS Specific Operations Risk Assessment).

## 1.5 References

SAE J3016 Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems

SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

SAE ARP 4754 Guidelines For Development Of Civil Aircraft and Systems

ASTM TR1-EB Autonomy Design and Operations in Aviation: Terminology and Requirements Framework

ASTM TR2-EB Developmental Pillars of Increased Autonomy for Aircraft Systems

ASTM TR3-EB Regulatory Barriers to Autonomy in Aviation

Proud, Ryan W., and Jeremy J. Hart. 2005. "FLOAAT, A Tool for Determining Levels of Autonomy and Automation, Applied to Human-Rated Space Systems" in Infotech@Aerospace, American Institute of Aeronautics and Astronautics (AIAA) 2005-7061. Arlington, VA: AIAA.

From Here to Autonomy: Lessons Learned from Human-Automation Research, Mica Endsley, 15 Dec 16

Autonomy Research for Civil Aviation: Toward a New Era of Flight (2014), National Research Council

EASA Artificial Intelligence (AI) Roadmap: A human-centric approach to AI in aviation

EASA First Usable Guidance for Level 1 Machine Learning Applications – Issue 1

ICAO Doc 10019 Manual on Remotely Piloted Aircraft Systems (RPAS)

International C2 Journal, special issue, volume 1, number 2, 2007, in "Automation Architecture for Single Operation, Multiple UAV Command, and Control (Cummings, Bruni, Mercier, and Mitchell)."

H. A. Abbass, J. Scholz, and D. J. Reid Eds., Foundations of Trusted Autonomy, Studies in Systems, Decision and Control, Springer Nature, London, UK, 2018.

A. Finn and B. Mekdeci, "Trusted Autonomy", Report no. DASI-AF-2014-009, University of South Australia - Defence and Systems Institute, Edinburgh SA, Australia, 2014.

R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, vol. 30, pp. 286-297, 2000.

T. Kistan, A. Gardi, and R. Sabatini, "Machine Learning and Cognitive Ergonomics in Air Traffic Management: Recent Developments and Considerations for Certification," Aerospace, vol. 5, p. 103, 2018.

N. Ezer, S. Bruni, Y. Cai, S. J. Hepenstal, C. A. Miller, and D. D. Schmorrow, "Trust Engineering for Human-AI Teams," Human Factors and Ergonomics Society 63rd Annual Forum, HFES 2019, Seattle, WA, USA, 2019.

S. M. Dambrot, D. De Kerchove, F. Flammini, W. Kinsner, L. MacDonald Glenn, and R. Saracco, "Symbiotic Autonomous Systems White Paper II", IEEE Symbiotic Autonomous Systems (SAS) - a Future Directions Committee (FDC) Initiative, 2018.

R. Saracco, R. Madhavan, S. M. Dambrot, D. de Kerchove, and T. Coughlin, "Symbiotic Autonomous Systems White Paper", IEEE Symbiotic Autonomous Systems (SAS) - a Future Directions Committee (FDC) Initiative, 2017.

J. Chevallier “Enabling Autonomy in Commercial Aviation: An Ontology and Framework for Automating Unmanned Aircraft Systems (UAS)”, MIT Graduate Thesis, 2021.

# 2. Overview of Automation in Aviation

## 2.1 Deciding Typology of System Automation

In modern transportation, numerous groups have attempted to lay out the groundwork for describing and defining the roles of humans and machines in performing tasks. Transportation is no exception to this trend with various classification schemes posed by academia, regulatory bodies, industry, and jointly through standards development organizations (e.g., ASTM, NIST, SAE, NASA, NRC – see 1.5 References). While each proposal provides value, they have all met challenges and criticisms in conceptual development or application. They all agree that discussions around automated and autonomous systems can become counter-productive when terminology is not well understood, and a common framework is not utilized.

Automation (see Definitions) within traditional aviation has progressed in various forms since the beginning of modern aviation. Automation is a way of designing functions that can be applied at all different levels of the system. Automation is not something new or dangerous: traditional aviation and many other industry domains already broadly implement automation. Examples can be found in most aircraft design domains, from stability augmentation systems on helicopters to full authority digital engine controllers on jet engines, flight management systems on commercial aircraft, and ground collision protection systems on fighter jets. This breadth of technological complexity and scope underpins the need for a flexible framework for designing, evaluating, and approving automated systems. Within the UAS industry, this need is compounded by having high levels of automatic function in even the most straightforward operational environment. Finally, automation can be used for both the UAS and the external environment in which the UAS is operating. These two domains interact more for UAS operations than for traditional aviation. To take the maximum benefit of the advanced technologies supporting unmanned aircraft, the degree to which the UAS operation is automated may be higher than in traditional aviation.

Autonomous systems (see Definitions) within traditional aviation have been limited to functions where human control is not possible (e.g., flight control of statically unstable aircraft). In traditional aircraft, the pilot is an essential part of the aircraft operation, following well-defined, well-understood, and well-communicated operational procedures and has demonstrated competency in these areas. However, as advancements in technology move beyond statistical machine learning (e.g., Bayesian networks, convolutional neural networks) to explainable causal symbolic models, artificial intelligence that can generalize to situations not found in training data sets allow for more flexible systems responses to a variable environment, opportunities to deploy robust autonomous systems are beginning to become viable. There are currently several ways of understanding autonomy. For example:

- Autonomy, as discussed in this document, is an emergent effect of a collection of increasingly automated functions. As the level of automation increases across a set of interacting functions autonomy may emerge; and
- There is an alternate vision of some approaches for autonomy based on the "non-deterministic nature" of data driven AI-based automated systems. The designer can predict the behaviour of a deterministic system if the inputs to the system are known. However, a non-deterministic system may exhibit behaviour that cannot be expected based on the inputs alone; they may involve concepts such as artificial intelligence (Bhattacharyya et al., 2015; Rierson, 2013).

Those concepts for autonomy may be similar in many, or even most, situations but may be contradictory in specific cases. Of particular note, automation and autonomy should be evaluated differently in the systems functional context and operational context, as autonomy is most often used in the operational context, and automation is used in both.

## 2.2 Stating Operational Assumptions

Discussion of automated operations must be understood in the broader context of the aviation safety system. As such, assumptions around key operational concepts should be evaluated regarding the technical environment in which the operation is being conducted:

Airspace Control Environment: The airspace system and air traffic services provided to the operation must be well defined and articulated. This is especially important to consider to manage air traffic separation. Of particular consideration is the information environment on which the operation depends and the extent to which it is automated.

Cybersecurity: One of the significant risks to autonomous operations is cyber threats. As systems become increasingly automated/autonomous the need to ensure only authorized personnel access the systems, and that systems are designed to be robust and resilient to cyber threats becomes the paramount concern. Therefore, cybersecurity has to be a fundamental tenet of the design and operation of all aircraft, airspace, and automation systems.

Levels of Service: Different airspace operations will have different dependencies on the available aeronautical information services. Each service (e.g., in a UAS Traffic Management environment) will have a level of service (e.g., technical capabilities, geographic coverage, assurance, integrity, etc.) available to the operators. Each operator will need to subscribe to services prescribed by the airspace manager (e.g., ANSP, CAA) and required for their particular operation. Unfortunately, there is no single relationship between increased automation and service levels. Instead, each aeronautical service has to be assessed as to its impact on the safety of a particular operation with a specific aircraft (e.g., Sustained Aircraft Manoeuvre Control becomes more automatic, the dependency on C2 services may be reduced, but the reliance on Detect Alert and Avoid (DAA) services may be increased).

Human Centric Automation: The central role of the human in the aviation system is recognized by many regulations, which codify the responsibility of individuals to do or not do certain actions or ensure that certain actions or results are achieved. The nature of these requirements may change depending on the technology being used, but the level of responsibility does not. As automation of operations and the airspace is addressed the key defining factor between functions is what role the human plays in planning and accomplishing tasks and how the human interacts with the machines in order to support safe operations. Human centric automation requires systems be carefully designed to support the human tasks and decision making in accordance with defined roles and responsibilities (e.g., emergency management, passenger safety).

Function Centric Evaluation: It is noted that although several of the existing automation level frameworks focus on system level definitions of automation and autonomy, this document looks at automation through a functional lens. Although system level definitions are useful for top level discussion, they are unable to represent the complexities of specific system architectures, and therefore are of limited use for structured analysis, safety assessment, and functional assurance. Systems will inevitably be comprised of a high number of functions, each of which may be operating at different levels of automation, therefore assigning a system level value will be difficult or misleading. The application of a leveling framework that is applicable at an individual function level can then be applied at higher levels of functional abstraction, e.g., collections of functions, system of systems.

Trustworthy Automation: For automated functions to enable the off-loading of tasks from crew, the humans need to trust that the automation will perform tasks as expected and return results in a consistent manner. Building trust in automation relies on robust design processes that adhere to appropriate safety assurance processes commensurate with the safety criticality of the tasks that are planned to be off-loaded. The level of trust must be established through functional testing and clearly understood by the people who will be expected to off-load tasks to the automation. This level of trust can only be achieved in conjunction with training (of pilots, decision makers and everyone involved in assuring the safety of the operation) to understand the limits of automated systems.

<u>Ethical Decisions</u>: The autonomous system or highly automated system follows codes of conduct that ensure an automated system can respond to situations within a generally accepted decision-making framework prioritizing aviation safety.

# 3. Methodology to Evaluate Automation Impacts

## 3.1 Defining Levels of Automation

There is a wide variety of UAS that will operate in the aviation system, from simple mechanical aircraft (such as model airplanes) to very advanced computer-controlled aircraft (such as high-altitude-long-endurance military drones). These aircraft systems have numerous capabilities, including navigation, communication, caution, and warning systems, each of which may have different levels of technology as part of their design and operation. In addition, these aircraft are integrated into complex airspace, and operational environments with varying levels of technological capability deployed to help manage the operations efficiently and ensure safety. As a result of this complex and varied environment providing a single classification scheme for automation, levels is, at best, exceedingly difficult.

To handle this problem a mechanism to describe the operational boundary in which a particular system or function has been designed to operate is required. The concept of the Operational Design Domain (ODD) fulfils this requirement. By defining an ODD, a designer, operator, or regulator can evaluate the capabilities of an airspace system, a specified UAS operation, a particular UAS, or even a subsystem or function within a UAS. While the definition of an ODD is a valuable tool to classify a specific design, it should be used carefully noting that most modern aircraft are highly integrated platforms with many modes of operation and a wide range of capabilities depending on which systems are available to provide information; as a result, aircraft may employ different levels of automation for the same task in other contexts. For example, altitude control or thrust control are typical examples of automated functions in traditional aviation. The limits of these functions may be operationally dependent and may be updated via software (through well-defined configuration control and change management processes) to change capabilities between missions. Careful consideration of the ODD both within the automated function and in relation to the operation helps communicate the safety impacts of these types of changes.

The ODD is necessary to help clarify complex functional dependencies. For example, it is challenging to describe the level of automation of the "follow-me-mode", as this capability may be achieved by a collection of multiple functions at different levels. The ODD allows the description of the various parts of the operation (e.g., sensing the human, controlling the flight dynamics, responding to obstacles) to be described at their individual levels of automation, while the “follow-me-mode” function would operate at a potentially different level of automated control.

It is recognized there are many external systems (e.g., UAS traffic management systems) which support a particular UAS Flight Operation, and these systems come together to form the broader aviation system. This infrastructure needs to be in place to support fully automated operations. Therefore, when developing a safety case utilizing automation, the composite airspace system in which processes occur will need to be assessed, including UAS flight operations, UAS, traditional aircraft traffic management, and ground support systems. It is expected that a similar classification as presented below may be used, but this will be addressed in subsequent JARUS documentation.

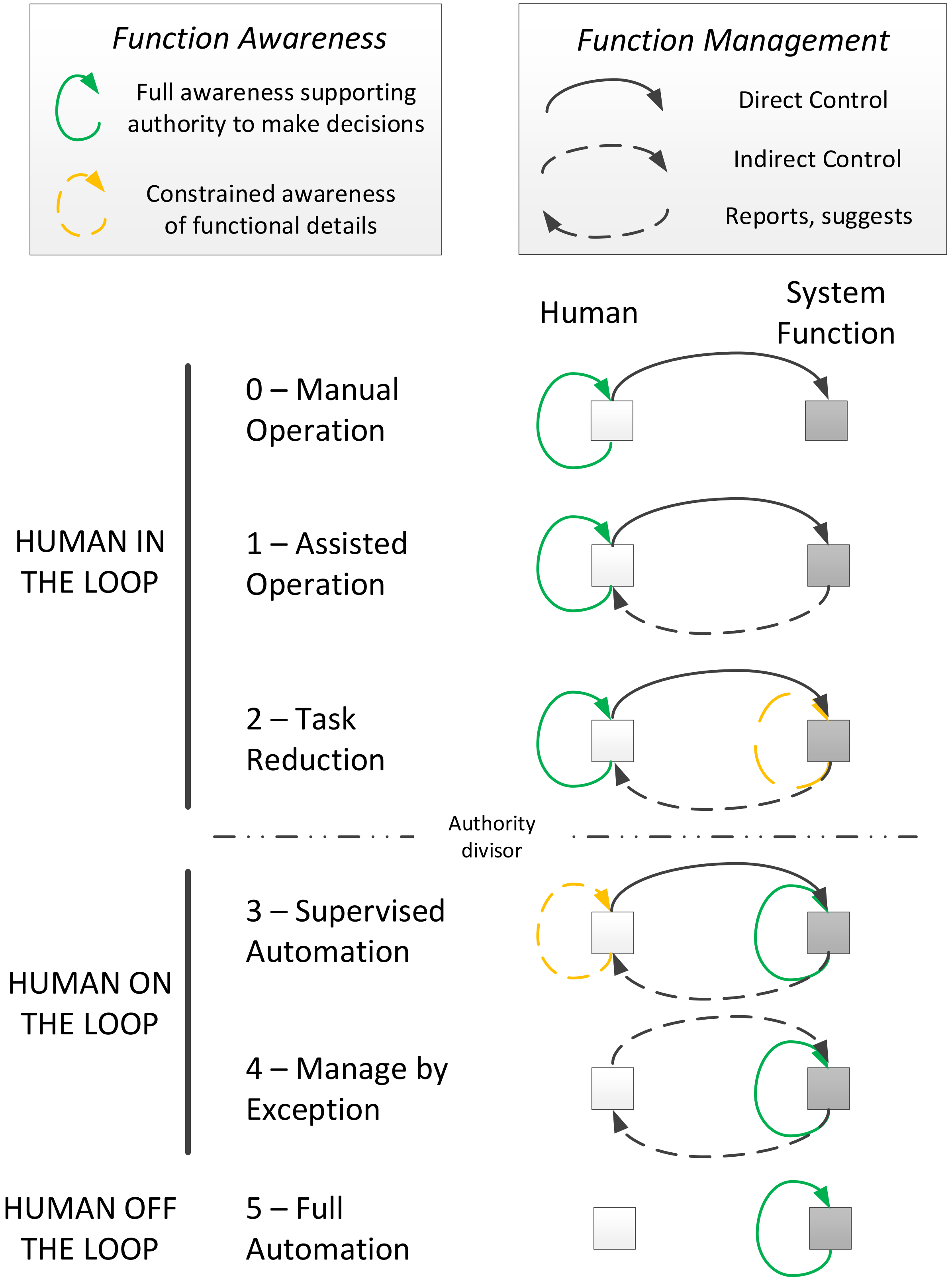
The primary purpose of this section is to provide a high-level framework for the ODD of UAS flight control. Still, from airworthiness and operational perspectives, many other functions will also be automated, and the challenge is to make all this automation work safely together. Therefore, this document describes the levels of automation as a spectrum focused on the human-machine team managing the flight of the UAS; namely: who has control of the aircraft flight and communication systems, how the aircraft interacts with the environment (external and internal to the UAS), and what happens when a failure occurs during flight. It is understood that the conceptual limits of the levels defined herein may not be achievable at the current state of technology, nor without risk or safety mitigations which national authorities may apply in conjunction with their risk-based analysis and approval of operations. Instead, the levels attempt to provide valuable milestones along a continuum of decreasing human intervention in flight operations, which can help guide discussions about what may be acceptable for certain operations, or within specified design domains.

In developing the basis for autonomous UAS concepts of operations, several core assumptions around traditional aviation operations have to be challenged regarding the airspace, design approval, and operational approvals. For the scope of the discussion below the following assumptions are made:

1) All air vehicles will interoperate (Mixed traffic – Traditionally operated and UAS where the rate of encounter may vary by type, including automated capabilities from low level automated advanced air mobility to high altitude platform system operations);
2) No human flight crew may be present on-board the UA to control the aircraft flight path or communicate with external systems, though there may be humans on-board with defined responsibilities to support safe operations (e.g., emergency management, passenger safety);
3) Operations will vary from low risk "open-field" operations with no or few people on the ground to higher risk operations over high-density urban environments;
4) ODDs will require a level of safety assurance and integrity related to the risk they pose during the operation determined by their specific functional criticality; and
5) To operate an autonomous aircraft, the air/ground management systems (equipment, personnel, and organizational) are proven resilient, proficient, and capable of supporting autonomous operations.

Below is a pictorial view (Figure 1) of the proposed levels of automation depicting how a UAS function may be achieved between the human and machine. It describes which part of the team has awareness of how the system function is being achieved along with the degree to which the entity with authority for performing the function can directly affect its execution. The methods of control in Figure 1 can be applied to all levels of functional aircraft components, which allows for an evaluation of available automated interconnections and system-level safety evaluations, but focuses on the nominal case (i.e., contingency management becomes more complex depending on aircraft design).

*Figure 1 Automated methods of control*



As depicted by the Authority Divisor horizontal line in Figure 1, Levels 0[1], 1[2], and 2[3] have the human in control, Levels 3[4], 4[5], and 5[6] have the machine in control.

This scale introduces full automation as the ultimate extension of functional automation. Within the context of this document autonomy, as an emergent property of functional automation, can be defined in reference to the framework for levels of automation and hence the requirement for interaction with a human supervisor. Full automation at a function or system level occurs when a human supervisor is not required (or able) to interfere. Applied to flight control, this type of functional automation links autonomy to a "human-off-the-loop" control scheme to understand that the human operator has no control or visibility on the automated functions. However, the human may have indirect operational inputs to the fully autonomous aircraft function by interacting via higher-level functions (e.g., mission planning). The difference in these levels is determined by the role of the human in authority over the execution of the function as well as how the human is engaged in the event of abnormal operation. The two major aspects driving the differentiation are:

> Human-Machine Teaming: Describes the relationship between humans and machines performing tasks as automation increases.
>
> Fallback: Describes how the UAS responds to a failure and where control of the function is expected to reside. Fallback is triggered when specific metrics associated with the operation of the system exceed the defined thresholds for safety. In a multi-aircraft supervised operation, for example, the crew may be passively monitoring the operation (not monitoring each individual aircraft in an active way but monitoring how the operation is being carried out). It is recognized that the fallback from complete system control to human control is difficult if the human has not been tracking the flight status or been provided some meaningful human control of the operation; as a result, knowledge of the state of the aircraft and communicating the airspace situation to the human crew is a driving design condition. This fallback function has the potential to create new hazards not traditionally captured in less automated functions. In the event of a failure that causes the human to intervene in managing the safety of the flight, the machine and the human crew will be working to solve issues and manage the functions to ensure the safety of the operation (e.g., pilot alerting regarding degraded operational modes), but responsibility for absolute control must always be unambiguous. When degraded modes affect air traffic management functions, systems, equipment, and personnel will need to understand how these contingencies can be safely absorbed into the airspace. This entails significant training, maintenance, and organizational impacts to traditional air traffic management. As operations become more complex, air traffic management functions may become increasingly automated.

Additional considerations for each of the levels of automation are described in the following subsections along with examples (UAS Control Airspeed and Mid-Air Collision Avoidance) to illustrate how the same functions may present at different levels of automation.

---

[1] 0 - Manual Operation: e.g., Pilot flying a model aircraft only by visual reference. No Instruments available.

[2] 1 - Assisted Operation: e.g., Pilot flying a model aircraft with key aviate instruments presented at the GCS.

[3] 2 - Task Reduction: e.g., Pilot flying a model aircraft with stability augmentation (i.e., Autopilot tries to damp out the effect of turbulence.)

[4] 3 - Supervised Automation: e.g., Pilot monitoring a UAS flying a pre-programmed survey route.

[5] 4 - High Automation: e.g., Pilot monitors as UAS flies a pre-programmed route and the UAS has the capability to tactically adjust that route as required to avoid obstacles.

[6] 5 - Full Automation: e.g., UAS oversees all aspects of the operation including the decision to go flying in the first place.

*Table 1 Automation Level of an Individual Function Supporting UAS Flight Operations*

| **Level**<br>**Criteria** | **Level 0** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** |
|---|---|---|---|---|---|---|
| | **Manual Operation** | **Assisted Operation** | **Task Reduction** | **Supervised Automation** | **Manage by Exception** | **Full Automation** |
| Human-Machine Teaming | Human led | Human-In-the-loop | Human-In/On-the-loop | Human-In/On-the-loop | Human-On-the-loop | Human-Off-the-loop |
| Fallback (Integrity Thresholds Exceeded) | Human | Human | Human | Human | Fall back Ready Human (Operator/ATS) | Machine (Limited or Segregated Operations) |
| **Level**<br>**System Function Examples** | **Level 0** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** |
| Sustained Aircraft Maneuver Control | Human | Human *AND* Machine | Machine (Managed by Human) | Machine (Supervised by Human) | Machine | Machine |
| Object and Event Detection and Response (OEDR) | Human | Human | Machine (Managed by Human) | Machine (Supervised by Human) | Machine | Machine |
| Communication with External Systems (Ground and Airspace systems) | Human | Human | Human *OR* Machine (Managed by Human) | Machine (Supervised by Human) | Machine | Machine |

Note: Most modern aircraft are highly integrated platforms with many modes of operation and a wide range of capabilities depending on which systems are available to provide information; as a result, aircraft may employ different levels of automation for the same task in other contexts.

### 3.1.1 Level 0 – Manual Operation

At the start of the automation continuum are Level 0 or "manual operations". Within the specified functional ODD, the human manually executes the function, receiving no support from the machine. It should be noted there are very few truly manual functions at the lowest level of ODD focus (e.g., there is a feedback circuit in the servo of the model airplane that tries to hold the control surface at the commanded deflection). Examples of L0 functions and systems include direct servo-controlled model aircraft and legacy general aviation aircraft (Piper J-3 Cub).

For the UAS Control Airspeed example, the function operating at L0 would have manual control of the throttle / RPM by the pilot with no measurement of airspeed; airspeed control is based only on the visual judgement of the pilot.

For the Mid-Air Collision Avoidance example, the function operating at L0 would have the pilot detecting the conflict, tracking and predicting the other aircrafts movement and manually executing any required avoidance manoeuvre based on relative position, flight paths, local airspace environment, and rules of the air.

### 3.1.2 Level 1 – Assisted Operation

Functions automated to this level are used to support the in-the-loop crew in performing the functional tasks. At this level of automation, the machine operates in an out-of-the-loop supporting role to the human in executing the function. The human still leads execution of the function, but within a clearly bounded ODD the machine would be able to offer limited support, e.g. provision of relevant information. . Examples include terrain awareness and warning systems (TAWS), and assisted take-off and landing for UAS.

For the UAS Control Airspeed example, the function operating at L1 would have the system provision of current airspeed and min / max limits. The pilot uses the provided info to adjust throttle / RPM to control airspeed.

For the Mid-Air Collision Avoidance example, the function operating at L1 would have the system provision of supporting information, e.g., alert (visual / aural) indication of a potential conflict and broad indication of direction. The pilot is then required to confirm the conflict, predict the other aircrafts movement, and manually execute any required avoidance manoeuvre based on relative position, flight paths, local airspace environment and rules of the air.

> Note: The interactions between functions at this level of automation and other functions which may be at different levels of automation need to be very carefully considered. When the crew is in-the-loop the system may suggest manoeuvres, and the crew may take this into account when deciding what action to take retaining meaningful control when executing the specific function. Thus, the crew and the system are working together to manage the flight operations.

### 3.1.3 Level 2 – Task Reduction

At this level of automation, control and monitoring are shared between the human and the machine. The machine now takes on an in-the-loop management role for the function, helping to reduce the human workload and / or skill level required to accomplish the task. The human still leads execution of the function, but within a clearly bounded ODD the machine now provides more significant level of support.

Examples of task reduction technologies include system failure alerts, air traffic control visualization systems, and obstacle detection.

For the UAS Control Airspeed example, the function operating at L2 would have the pilot directly commanding airspeed, and the machine controlling RPM / throttle as required to meet the pilot demand.

For the Mid-Air Collision Avoidance example, the function operating at L2 would have the system provision of supporting information and advice, e.g., conflict alert and resolution advisory based on predicted flight paths, local airspace environment, and rules of the air. The pilot needs to validate the provided information and execute the avoidance manoeuvre.

> Note: The human crew may be either in or on-the-loop for this function depending on the nature of both the scoping ODD and the architecture of the specific system. The expectation is that the crew can intervene and override the automated system at any time providing meaningful human control of the functions outcome. The machine generally performs the steps to accomplish the function and the human directs or validates the system actions at a higher level. When the design has the crew on-the-loop, the machine performs some aspects of a function without crew action.

### 3.1.4 Level 3 – Supervised Automation

At this level of automation, the machine executes the function under the supervision of the human who is able to monitor and intervene with the operation at any time. A critical distinction between this level and lower levels of automation is the human is not aware of the internal states regarding the execution of the function, but rather is supervising the outcomes and intervening as they determine necessary to manage the safety of the function. Although the machine now leads the execution of the function (under a clearly parameterized ODD), the human is required to continually monitor the output of the function and must be provided with sufficient information and ability to maintain awareness to be able to intervene as preferred, e.g., for either flight safety or function effectiveness. This requires careful human factors system design to ensure that the human has all the required information to go from "on-the-loop" to "in-the-loop" when required. Examples include an automatic traffic collision and avoidance (TCAS) system tied to an autopilot which can automatically perform a manoeuvre when a Resolution Advisory is alerted, and AI-enabled UAS that automatically avoid fixed obstacles, even during piloted flight.

For the UAS Control Airspeed example, the function operating at L3 would have the machine defining the airspeed command, as appropriate for the particular mission phase, under the supervision of the pilot who is able to monitor, intervene, and set a new airspeed command if preferred.

For the Mid-Air Collision Avoidance example, the function operating at L3 would have the machine detecting the conflict, tracking and predicting the other aircraft's movement, and executing any required avoidance manoeuvre based on sensed relative position, flight paths, local airspace environment, and rules of the air. The pilot is informed of the situation at all times, and is able to monitor the automated response, intervening and adapting the system response as preferred.

> Note: At this level of automation, the human crew is on-the-loop actively monitoring the function. The automated functions are also actively monitoring themselves to provide the crew with awareness of function performance and system status. The human is supervising the automated functions and maintaining awareness of the operational parameters to provide meaningful human control over the outcomes of automated functions.

### 3.1.5 Level 4 – Manage by Exception

At this level of automation, the machine executes the function, alerting the human in the event of an issue. The key distinction from lower levels is the human is no longer required to continually monitor the function in real time. However, the human is now required to be available and able to intervene at any time after being alerted by the machine to an issue. Once the machine has demonstrated the ability to perform entire functions effectively and have a robust capability to respond to the environment, the crew may trust the machine to operate without human supervision (within a specified ODD). Demonstrating this ability requires gaining a level of trustworthiness (e.g., for data driven AI-based methods, EASA First Usable Guidance for Level 1 Machine Learning Applications – Issue 1) in the particular implementation which demonstrates the ability of a solution to meet safety (reliability, integrity, and assurance) expectations. One system level example is the "drone-in-a-box" autonomous surveillance system.

For the UAS Control Airspeed example, the function operating at L4 would have the machine defining the airspeed command and monitoring the actual airspeed against pre-defined limits. The pilot does not actively monitor airspeed, but the function alerts the pilot in the event of a pre-defined limit being breached, e.g., too fast or too slow.

For the Mid-Air Collision Avoidance example, the function operating at L4 would have the system detecting the conflict, tracking and predicting the other aircrafts movement, and executing any required avoidance manoeuvre based on sensed relative position, flight paths, local airspace environment, and rules of the air. The pilot is only informed of the manoeuvre in the event of pre-defined conditions being met, e.g., predicted minimum separation limit breach, or difficulty tracking the intruder aircraft to a required level of accuracy.

> Note: At this level of automation, the human crew may be either on or off-the-loop (though in cases where the human is on-the-loop their role is as monitor and have no direct interaction until tasked by the machine), depending on the design of the system and the scope of the ODD. The crew only intervenes when the system is in a fault/fail state and the machine has determined a need for human intervention, but the crew is not actively on-the-loop monitoring flight status. With the machine taking over execution of the function, the crew maintain meaningful human control less over operational objectives and more usually at a strategic level (e.g., through pre-flight planning, monitoring of operational performance) and in coordination with other functions (which may be automated to various levels).

### 3.1.6 Level 5 – Full Automation

At the far end of the spectrum is a fully automated function. At this level of automation, the machine is fully responsible for function execution, and the human awareness of dynamic operational parameters is limited or non-existent. At this level, the human interaction with the machine is generally limited to providing high-level strategic directives (e.g., pre-flight planning or tactically though high-level system management) and observing resulting outcomes. Further, the human without special authority is unable to intervene in real-time either due to practical limitations or deliberate exclusion within the ODD. It is expected that these types of operations can only be achieved through the leveraging of advanced technologies (e.g., Artificial Intelligence) or by tightly scoping the ODD to bound the operation of the autonomous function. An ODD (e.g., airspace operational limitations) will be applied by bounding the operation through interactions with the broader functional system (e.g., segregated airspace operations), these functional bounds allow for the limitation of necessary human interaction. For example, the UAS may be Level 5, but the external environment where the UA is operated may have a lower level of automation. An example of this type of operation would be autonomously launched and managed high-altitude communications balloon networks.

For the UAS Control Airspeed example, the function operating at L5 would have no expectation for pilot monitoring or intervention in airspeed control at any stage of the flight.

For the Mid-Air Collision Avoidance example, the function operating at L5 would have no real-time interaction between a pilot and the avoidance manoeuvre. Any events or issues may be reviewed / analysed post-flight.

### 3.1.7 System Function Examples

In the context of flight operations, many functions work together to ensure the safety of flight. Applying the levels of automation to UAS flight operations also requires the consideration of how the system will aviate, navigate, and communicate in the airspace. As a result, the following additional aspects of the flight operation are discussed to help support descriptions of concepts of operations in a particular airspace and are summarized in Table 1.

Sustained Aircraft Manoeuvre Control: Describes how the aircraft is controlled (e.g., crew inputs) and systems are monitored (e.g., fuel level monitoring) as tasks are automated. Throughout the automation spectrum the functions related to operation of the aircraft within a specified ODD may be performed by either the human crew or the machine.

Object and Event Detection and Response (OEDR): Describes how the aircraft interacts with the environment in which it is present and how it may respond (e.g., detect and avoid failure monitoring). Events may occur on-board the aircraft or may be external and communicated to the mechanism responsible for sustaining aircraft manoeuvre control. When the ODD is expanded to include evaluation and response to environmental variables (e.g. collision hazards, other aircraft, and weather events) the machine may be given more abstract goals/commands (e.g., find the most fuel-efficient route, remain well clear) as compared to a more simplified directive (e.g., follow this route).

Communication with External Systems (Ground and Airspace systems): Describes how the UAS interacts with the external systems in which it is operating (e.g., ground crew, ATC). The nature of the external system will depend on the nature of the operation being conducted in the airspace. It is envisioned UAS will interact with external systems if such systems exist. It is recognized a UAS may be able to communicate with external systems with very little human oversight (e.g., ADS-B position reporting) though it depends on both the function and bounding ODD, as well as the design of the airspace systems including air traffic management and information services. The automated functions of the airspace system will need to be well understood when integrating the operation as the airspace systems may need to accommodate for multiple levels of automated communication functions.

As an example, the external system may provide inputs/requests to the UAS if necessary; the external system will collaborate with the flight system to support safety objectives (this goes beyond the exchange of information as, in most cases, an external safety layer will be needed to mitigate out of control operations). In this case the operation will need to be constructed to consider the entirety of the airspace and make decisions to maximize safety. The automation of the airspace environment will be considered in a future JARUS document.

When interacting with air traffic control systems various questions need to be considered when automating functions that impact air traffic management. These tasks will be addressed in a future JARUS document, and include:

- What safety risk does the task mitigate, and how is it coordinated with other airspace users?
- How does the aircraft communicate the operational intent?
- Who do I need to contact, and how to coordinate planning when in degraded modes of operation?

## 3.2 Describing Functions and Safety Dependence

While the high-level ODDs described above are a good starting point for evaluating operations as they are broken down into functional blocks the level of automation may become harder to discern (e.g., is the OEDR function realized in whole or in part by external ground systems?). Therefore, to better understand the operation, the ODDs may be refined into high-level functions to more clearly understand how each part of the system is automated and whether it meets the criteria for the levels described above. These functions are not standalone, and many of them depend on the function and reliability of each other, as well as the configurations of the other systems in the operational environment (including people supporting the operation). To understand how the safety of the operation can be fully assessed, these dependencies need to be defined and described. The dependencies help communicate how the automated functions work together and where the highest areas for risk may lay with a particular operation. An example breakdown and dependency analysis is provided in Appendix A – ODD Functional Decomposition. While there may be a high level of automation for aircraft functions supporting systems, the operational context can limit the safety impact allowing their operation to be considered lower risk. Building on JAR Doc 09 ("UAS Operational Categorization") using the functional breakdown of the automated functions (such as Appendix A) and evaluating the independence of these functions, along with the hazards they pose, the effects of automation on the operation can be described based on their risk to safety.

Key to describing automation risk is understanding which functions are critical to the operational safety, which functions contribute to operational safety, and which functions do not impact operational safety. As a means of risk-reduction many functions have redundant systems (including humans) which help limit the impact of failures or incorrect function. Special attention should be paid to functions where the human may perform the function in event of failure, as a cumulative increase in workload (e.g., resulting from multiple system failures) may eventually lead to safety impacts and training skill requirements. Identifying the degree to which a particular automated function acts independently in supporting the safety of the operation allows for a more holistic view of the risks posed in an automated operation. While there are many methods of categorizing functional safety (e.g., SAE ARP 4761) the general categorization of functional independence is described as follows.

### 3.2.1 Safety Independent Functions

Automated functions can be considered as safety independent when those functions can be entirely accomplished by another means in the event of a detected failure or incorrect operation, and the failure of these functions alone do not directly impact the safety of others in the operational area (either in air or on ground). E.g., automated radio channel selection in a Category A operation.

### 3.2.2 Partially Safety Dependent Functions

Automated functions can be considered as partially safety dependent when the functionality would be reduced or degraded in the event of a detected failure or incorrect operation. This degree of independence requires that other systems be present to support continued operation of the system, but the failure of the automated function results in operational limitations in order to maintain safe flight. E.g., position precision augmentation to support geofence compliance in a Category B operation.

### 3.2.3 Safety Dependent Functions

Automated functions can be considered as safety dependent when the function cannot be accomplished by any other means in the event of a failure or incorrect operation, and the failure or incorrect operation of the function results in a direct impact to the safety of others in the operational area (either in air or on ground). This degree of independence requires the rapid identification of the failure or incorrect operation which triggers well defined emergency procedures. E.g., control surface actuator management in a Category C operation.

## 3.3 Describing the Impact of Automation

The broad spectrum of operations, aircraft architectures, and airspace environments in which UAS may be employed leads to the need for a flexible yet robust method to describe the impact automation has in a particular operation. When evaluating a function to determine the level of automation and the impact, it is essential to understand the expectations related to the capabilities being automated and their relationship to the air and ground environments in which they are operating. While automation is often framed as a risk mitigation (e.g., reducing potential for human error) this mitigation needs to be supported by well-balanced trust frameworks for product development and operational management, as increasing the level of automation does not on its own necessarily increase the risk of the execution of a function. To this end the level of automation of a particular function (as described above) can be combined with the safety dependence of that function to help assess the impact a particular function has on an operation. Table 2 describes the relationship between the safety dependence and the level of automation. It should be noted that existing aviation practices (e.g., JARUS Specific Operations Risk Assessment) at least implicitly address the safety impacts of levels 1 and 2, but the potential impact is described here for completeness.

*Table 2 Impact of Automated Function*

| | | Level of Automation | | | | | |
|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 |
| Safety Dependence | Independent | No Automation | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 |
| | Partially Dependent | | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 |
| | Dependent | | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 |

🟩 Low Impact
🟨 Medium Impact
🟥 High Impact

The impact of the automation does not in and of itself directly relate to a change in the risk of an operation, but the assessment help provide context for evaluating automation within the broader operational context. In general, as operational environments become more complex, there is a need to automate capabilities. Clarifying the dependencies amongst capabilities helps determine which are critical to safety and which are supportive of safety. It also helps explain the complexity of the aircraft and air traffic systems and whether the implemented automation will meet the expectations of the operators and safety managers. Unfortunately, as the complexity of operations increases so too may the risks of the operation relative to other means of operation (e.g., visual-line-of-sight (VLOS) infrastructure inspection vs. a “drone-in-a-box” beyond-visual-line-of-sight (BVLOS) inspection of the same infrastructure). This means as operators' expectations around automated capabilities rise, the requisite reliability of the automated capability rises and requires proportionate performance-based oversight by safety authorities. By understanding the impact of a particular automated function operator expectations can be balanced against the required oversight to ensure safe operations. An example of an impact evaluation utilizing the functional break down in Appendix A – ODD Functional Decomposition, can be found in Appendix B – Automation Functional Impact Assessment.

# 4. Considerations for Automation Frameworks

## 4.1 Developing Trusted Automation

Across the spectrum of automation is the goal of building trustworthy systems, independently objectively assessing their trustworthiness, and then calibrating justified trust between the machine and the human to achieve a highly autonomous system which can optimally interact with the human to deliver the highest possible levels of mission safety, efficiency and effectiveness. Across these levels, the UAS will operate autonomously and unsegregated from other flight vehicles (both conventional and autonomous platforms).

As the functions move to higher levels of automation, the underlying assumption is that the machine will perform adequately and safely in all normal operating conditions (outperforming humans, avoiding placing them in harm's way, or reducing required staffing levels). However, the exceedance of integrity thresholds (i.e., when the human or machine reaches the edge of its performance) would trigger a fallback function with selective allocations of responsibility to the human, the machine or their combination, assuring the maximum level of safety and performance achievable (the machine and the human support each other to maintain safe flight). It is expected that this level of operational integration will be based on a two-way and real-time monitoring of both machine and human integrity levels, achieved by intelligent health and mission management functions. Achieving this level of integration requires the careful application of trust frameworks (e.g., EASA Artificial Intelligence Roadmap for data driven AI-based methods) in both the development of the automated systems and the training of the humans. An example of such a relationship would be an automated landing system which monitors the health/responsiveness of the human pilot to determine if it needs to take control of the aircraft for an emergency landing.

Greater trust in an autonomous system facilitates approval of the system for more diverse and dynamic operations. Limited trust in an autonomous system may require limitations on the ODD approved for system operation. Trusted automation can be considered a pathway to progressively remove the inherent limitations of full automation as known today (e.g., furthering trust in the emergency landing system described above could allow for the human to delegate authority outside of emergency scenarios).

An example of automating the "UAS Create Flight Plan" task is outlined below with increasing levels of automation requiring more measurement of both the aircraft systems and pilot performance. The trust in the automation is progressive over these successive levels.

- Level 0: Manual Operation: Pilot manually creates flight plan, e.g., via drawing waypoints on a map display. Pilot manually checks weather forecasts and calculates flight time, fuel levels, and any contingency plans.
- Level 1: Assisted Operation: Pilot manually creates the flight plan, and the function annotates this with supporting information, e.g., flight time and fuel usage based on latest weather. The pilot then assesses the provided info and adjusts the flight plan as required.
- Level 2: Task Reduction: The function creates a baseline flight plan that the pilot then needs to adjust for the actual tactical situation / environment, e.g., restricted areas, start / end times, height limitations, contingency plans, etc.
- Level 3: Supervised Automation: The function creates a flight plan with full awareness of forecast weather, airspace restrictions, contingency requirements, fuel, time, etc. The pilot supervises the plan and has an opportunity to approve / revoke the plan before it becomes active.
- Level 4: Manage by Exception: The machine creates and activates the flight plan, only reverting to the pilot in the event of a plan failure or other unexpected issue, e.g.,

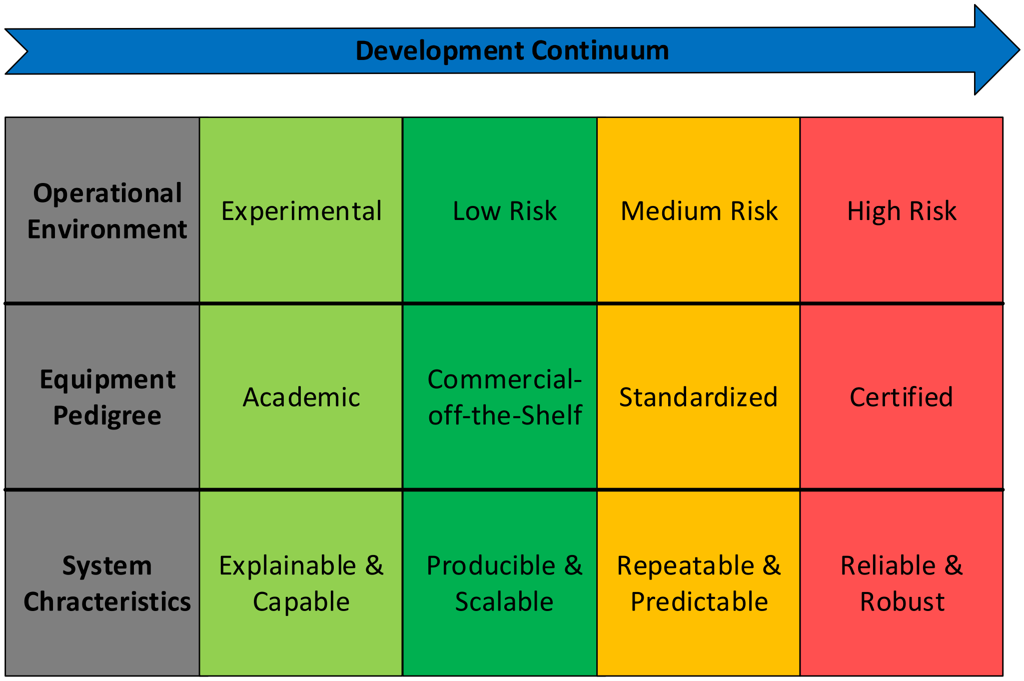
weather limit breach, airspace restriction, endurance limit breach, failed to find appropriate contingencies, etc.

- Level 5: Full Automation: No real-time interaction between a pilot & the plan. Any issues will be reviewed / analysed post-flight.

## 4.2 Assessing Technology Maturity

As automation fundamentally transitions from human-based operations to machine-based operations the technology used must be well understood. In addition, because of the potential impact on human lives, it must have a pedigree consistent with the risk of its usage. Innovation and experimentation with new technologies drive the automation of aviation functions but must be balanced against the oversight of design, production, maintenance, and scalable deployment. Considerations on how technology may move through development and deployment are illustrated in Figure 2.

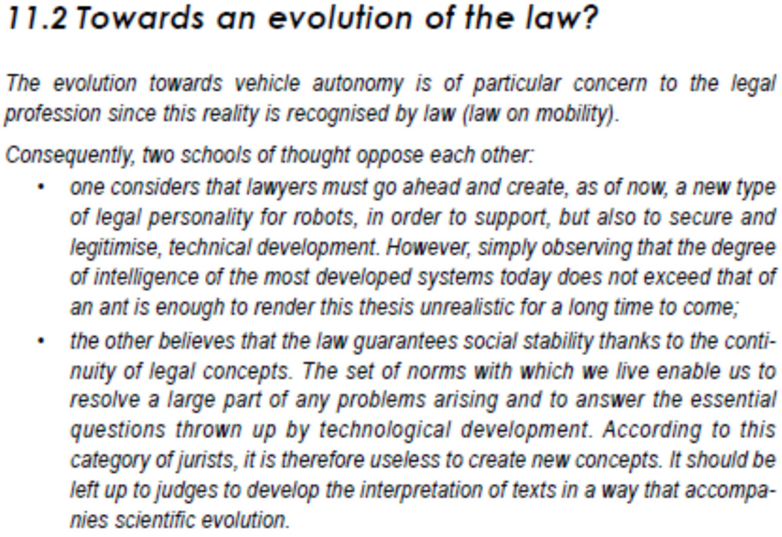
*Figure 2 Automated Technology Development Continuum*



| | | | | |
|---|---|---|---|---|
| **Operational Environment** | Experimental | Low Risk | Medium Risk | High Risk |
| **Equipment Pedigree** | Academic | Commercial-off-the-Shelf | Standardized | Certified |
| **System Chracteristics** | Explainable & Capable | Producible & Scalable | Repeatable & Predictable | Reliable & Robust |

## 4.3 Considering Consequences of System Automation

While automation within aviation has been progressing throughout the decades, it has not always done so fully aware of the ramifications of the changes to the operational paradigm. Indeed, this is not always the case. The mosaic of concerns dealing with automation within a specific ODD cannot be fully captured within a single document. Still, the sections below attempt to outline three key areas where consequences of automation must be considered: Responsibility for designing, manufacturing, and operating the UAS, Authority to control the UAS, and Liability in the event of incidents. It should be noted that while this section discusses a framework for these areas, there is still developing debate around how to address highly automated autonomous vehicles within the varied global legal frameworks (e.g., Roman Law, Common Law). The resolutions of these legal definitions will be important in any regulatory implementation for automated aviation systems. This issue has been recognized by many international institutions including the French Academy of Air and Airspace (l’Académie de l’air et de l’espace, AAE), which concluded:



### *11.2 Towards an evolution of the law?*

*The evolution towards vehicle autonomy is of particular concern to the legal profession since this reality is recognised by law (law on mobility).*

*Consequently, two schools of thought oppose each other:*

- *one considers that lawyers must go ahead and create, as of now, a new type of legal personality for robots, in order to support, but also to secure and legitimise, technical development. However, simply observing that the degree of intelligence of the most developed systems today does not exceed that of an ant is enough to render this thesis unrealistic for a long time to come;*
- *the other believes that the law guarantees social stability thanks to the continuity of legal concepts. The set of norms with which we live enable us to resolve a large part of any problems arising and to answer the essential questions thrown up by technological development. According to this category of jurists, it is therefore useless to create new concepts. It should be left up to judges to develop the interpretation of texts in a way that accompanies scientific evolution.*

### 4.3.1 Responsibility

Within the context of UAS operations, responsibility pertains to who (the human or the machine) performs which actions to manage the flight operation safely. As automation increases, there is an increasingly shared responsibility between the machine and the human operators. As a result, the responsibility for the safe operation of the UAS has been allocated to the various actors involved with developing an approved UAS operation, namely: UAS designers, manufacturers, operators, pilots, and approval authorities.

Designer: The designer is responsible for developing a safe UAS design. The designer also communicates the operational limitations of the system, including the defined and tested flight envelope (usually through a Flight Manual or similar document).

In traditional aviation, regulators have traditionally developed prescriptive sets of rules imposed on designers to develop safe systems. Industry standards have been used to help designers assess the safety of the developed systems and put in place development assurance activities to limit the likelihood of errors in software or airborne hardware. It is recognized that, for UAS, such an approach cannot address the varied designs and implementations. As such, the industry standards used in traditional aircraft design may not be immediately applicable to unique features of a particular UAS design. If no specific design standard exists (or is mandated) for a feature or system the designer still designs according to more generic available standards. It is generally recognized that increasing levels of automation may give the impression of higher complexity despite a very deterministic behaviour of each system taken individually. This may request new design standards, which could be different as the levels of risk increase.

For Levels 0 to 3: The design and operations will determine the standards needed to meet design and quality assurance.

For Levels 4 and 5, because humans are not necessarily in-the-loop, designing following applicable standards should be mandated.

Manufacturer: The manufacturer is responsible for manufacturing the UAS following the design and the quality assurance procedures.

Operator: The operator is responsible for the safe operations of the UAS within the specified ODD through the development of standard operational procedures (SOPs), operations manuals, contingency planning, and risk management and safety management system (SMS) processes (as applicable). Any UAS (piloted, automated, and autonomous) operation must occur via an operators' authorization utilizing SOPs and SMS.

In addition, maintenance organizations develop maintenance programs according to the UAS maintenance manual, but the operator ensures all required maintenance has been performed on the UAS before the flight. The maintenance actions required will typically be based on the complexity of the UAS and the robustness of the design. Maintenance-based SMS processes may be required to account for smaller operators not having (or requiring) maintenance organizations.

Finally, as the level of automation increases, the operator has to ensure the tasks no longer assigned to the pilot are allocated accordingly across the operation (e.g., pre-flight aircraft checks may be performed by other ground personnel).

Airspace Management Personnel: As the level of automation of the operation increases, it must still integrate with the available and required systems to support air traffic management activities. To support integration, ATM personnel and systems may become increasingly automated. Airspace automation considerations will be addressed in another JARUS document.

Pilot: Increasing levels of automation have a tremendous effect on the duties associated with the pilot: as the level of automation increases, the pilot functions reduce:

> *Level 0*: The pilot is always responsible for the safe operation of the UA.
>
> *Level 1*: The pilot is always responsible for the safe operation of the UA. The pilot is in-the-loop to perform all safety functions—the automation assists with the safety function.
>
> *Level 2*: The pilot is always responsible for the safe operation of the UA. The pilot is in/on-the-loop (depending on the nature of the design) to monitor all safety functions when the automated functions are engaged.
>
> *Level 3*: The pilot is always responsible for the safe operation of the UA. The pilot is in/on-the-loop to monitor all safety functions when the automated functions are engaged. The pilot responsibility may be limited if all system functions are reporting as nominal and there is no other means to identify a need for pilot intervention (e.g., unknown malfunction on a Cat III ILS approach)
>
> *Level 4*: The pilot is responsible to perform an action when the automated functions hand over authority of the UA flight task. This is the most challenging case for the handover of responsibility between the automated function and the pilot. Therefore, UAS designed at this level of automation must consider factors related to human

situational awareness to provide for the best chance of continued safe operations.

*Level 5*: Not Applicable: Humans are off-the-loop. The autonomous system gets no assistance from humans to perform any function.

Approval Authorities: The approval authority is responsible for following the approval process and issue the UAS operational approval. The authority is also responsible for oversight of the operation, following their oversight principles. There may be multiple approval authorities involved in approving procedures and may include design, manufacturing, airworthiness approvals, training, etc.

### 4.3.2 Authority

The question of authority is one of the critical enablers in distinguishing automated from autonomous systems. Authority delineates which system (Autonomous System or Human) can decide and take action to manage the flight operations.

In the case of flight operations, authority is considered within three operational boundaries:

1. Normal: In which the UAS is operating within its defined operational limitations with no errors or failures;
2. Abnormal: In which the UAS is operating within its defined operational limitation but has encountered unexpected issues and may be engaging in contingency procedures (e.g., may need to manoeuvre outside of the expected flight path); and
3. Emergency: The UAS can no longer retain flight control or is in a non-recoverable/unresponsive state. In automation Level 4, when the machine hands over authority to the human, the system can be considered an emergency.

Each of these three operational boundaries is considered in conjunction with the level of automation described in this document, as depicted in Table 2 below.

*Table 3 Flight Control Authority at Different Levels of Automation*

| | **Authority** | | |
|---|---|---|---|
| **Level of Automation** | *Normal* | *Abnormal* | *Emergency* |
| *Level 0* | Human | | |
| *Level 1* | Human *AND* Machine[1] | Human | Human |
| *Level 2* | Human *AND* Machine | | Human |
| *Level 3* | Machine | Human *AND* Machine[2] | Human[3, 5] |
| *Level 4* | Machine | | Human *AND* Machine[4, 5] |
| *Level 5* | Machine[5] | | |

Note 1: This shared authority is design-dependent – the design will dictate to what degree authority is provided to the machine vs. the human and the degree may vary from function to function.

Note 2: This shared authority has the machine making the decision but allows the crew to override decisions.

Note 3: The human can always override the machine to manage the flight operations.

Note 4: Both the machine and human can manage the emergency. The machine will keep trying to recover the system, but the human has the ultimate decision to take over. Ultimate responsibility for the outcome lies with the human operator (as described above). The machine needs to declare the emergency as it has sole awareness of the system condition and authority to monitor and declare the emergency. The human has the authority (which may not be sole authority depending on the design of the system) to take any action within the bounds of the declared emergency (e.g., terminate flight, advise ATC and other airspace users of emergency procedures/manoeuvres).

Note 5: For cases where a superordinated authority (e.g., ATC) has responsibilities to ensure the safety of the airspace there may be emergencies which require them to provide direct or indirect commands to manage the emergency. The ability to do this will depend on the particular airspace design and the availability of supporting infrastructure.

### 4.3.3 Liability

Automation allows operators to benefit from all the new advanced technology available such as Artificial Intelligence, Machine Learning, Blockchain, etc. However, increasing automation creates some new technology-related safety and security concerns while resolving some human-related ones. One of the most sensitive questions is the role of the human in contingency situations for automated systems. The reversion to human control is a very complex handover, which must be carefully organized, which emphasizes the need for the sound implementation of human factors design principles for the machine and sufficient training and currency for the human operators.

Automation of systems has legal implications depending on the methods described above. Who is responsible in the event of a failure: Operator? Manufacturer? State? This document aims not to discuss the details of the legal aspects, but the sharing of liability in the case is linked to the automation method. Liability is a matter relating to how regulations are handled within different jurisdictions.

# Appendix A – ODD Functional Decomposition

This appendix describes one possible way of decomposing the five required operational capabilities into a functional architecture. This functional description helps explain which parts of the aircraft operation are automated and to what degree. The interdependencies between these functions and the degree to which they are automated helps identify whether the automation has a safety impact on the operation. It is recognized there are many ways to identify functionalities and represent their interrelations. This is one example of a functional decomposition and should not be considered authoritative.

## A.1 Human-Machine Teaming Capability Decomposition

Aircraft Control Handoff: Aircraft control is achieved through the manipulation of flight control surfaces and propulsion systems (and many other aircraft systems), which may be accomplished with a human-in-the-loop or not. As automation changes, the relationship between the human directing the aircraft operation and the machines manipulating the physical aircraft, identifying control authority, and handing over control of the physical aircraft systems must be considered.

System Status Awareness: Awareness of aircraft status, air traffic service, and supporting system status is key to operational and safety management of automated operations. Human awareness of the system status requirements and methods for determining equipment and system status need to be considered at each level of automation. In addition, communicating these statuses to impacted decision-makers (human or machine) needs to be considered.

Multiple System Management: Considerations for how a single operator may manage multiple aircraft concurrently during a single operation need to be developed for this document. When aircraft are mentioned, it may also refer to multiple aircraft in pre-planned and actively managed formations.

Tolerable Latencies: Latency between aircraft, ground systems, and other airspace users must be considered as well as human response times when evaluating operational risks and mitigation efficacy. Latencies between control commands and execution of the commands should be considered especially under failure cases and during contingencies (e.g., remain well clear/collision avoidance timelines).

## A.2 Sustained Aircraft Manoeuvre Control Capability Decomposition

Position Assurance: To manage a complex operational system, each aircraft must have a 4-dimensional position that can be shared internally and externally to support airspace management. It should include a 2-dimensional geographic reference (e.g., Lat/Long @ WGS-84), an altitude (e.g., Barometric Altitude), and a time reference (e.g., UTC) along with associated accuracy for each dimension. Ideally, these dimensions should each use a common reference within the airspace to avoid miscommunication and mishaps. However, multiple reference systems may be accommodated through large enough error tolerances for operations.

Common Navigation Reference: For an aircraft to be directed effectively, a pilot (human or machine) uses navigation references and own-aircraft to issue aircraft control commands. As automation levels increase and the communication between aircraft becomes more safety-critical, common position and altitude navigation references (e.g., GNSS coordinates, Radio Navigation aids) are essential in ensuring successful de-confliction of operations.

Dynamic Systems Coordination: As aircraft become more complex with varying system dependencies, redundancies, and state evaluations, the need to coordinate systems (e.g., through common timing references) becomes more critical. For operations to push towards higher levels of automation, the mechanisms around how aircraft, ground, airspace, and human systems are coordinated need to be evaluated. Aircraft and aircraft systems operating in isolation may not have sufficient information to make the safest decisions for the airspace system in which they are operating or may not have sufficient response time to react to changes in the system; as a result, systems coordination becomes increasingly important as functions are automated.

Flight Management and Operational Envelope Assurance: This capability describes how the aircraft is controlled and how the automation ensures it stays within the flight limitations described in the aircraft flight manual. Manipulation of the actual control surfaces of the aircraft to guide the flight path of the aircraft may be performed directly or through compensatory systems (e.g., mechanical, electrical, software) in response to the directives of the flight control system (human or machine). The aircraft's actual flight management has numerous systems, and subsystem components and may be divided into many different functions that may be automated to various degrees. As automation increases, humans become less and less involved in manipulating controls and less "connected" to the system states. However, to avoid putting the aircraft into dangerous situations, the limitations developed by aircraft designers (and regulators where appropriate) must be respected. Ensuring the aircraft does not exceed its flight envelope capabilities may be accomplished in several ways but must be addressed to ensure safety.

## A.3 Object and Event Detection and Response (OEDR) Capability Decomposition

Geographic limit and Airspace awareness: Knowledge of the airspace, environmental conditions, and ground environments are essential aspects of a flight's safety management. In general, geography and airspace are considered as part of flight planning. Still, it is recognized that the geographical and airspace environment may change dramatically during operation, especially for long-term flights. Maintaining awareness of the changes in these conditions (e.g., movement of large groups of people, temporary flight restrictions, NOTAMs) is crucial for completing the operation and managing contingencies to preserve safety. As the environment becomes more complex, the systems need to remain connected and have robust information sharing to ensure a complete picture of the operational environment can inform correct decision-making (e.g., operational restrictions due to weather changes, route management to maximize fuel efficiency). As operations near their defined boundaries, they depend on containment systems to keep the operation from posing more risk than desired. Containment systems offer a suitable means of reducing risks to adjacent people and airspace but must become more robust as the risk increases.

Terrain and Obstacle Avoidance: With remote pilots, the need for a UAS to detect, alert of, and avoid terrain and obstacles is well understood. As part of the flight planning phases, difficult terrain and obstacles should be identified, but in BVLOS operations, the planned and actual environment may not always align. As a result, as this capability (and sub-functions) is increasingly automated (e.g., through combinations of sensors and artificial intelligence), considerations around environmental awareness (e.g., actual environmental conditions) and communication of those changes to the broader aviation system need to be well understood, and risks managed.

Aircraft and Airborne Hazard Avoidance: DAA is a core function for all UAS. As the operation goes BVLOS the DAA capability becomes more automated. Aircraft separation is predicated on the capabilities of one aircraft to maneuver to avoid another conflicting aircraft; as automation takes on more of the DAA responsibility, the expectations around the specific aircraft maneuvers (and the handling qualities of the aircraft) need to be well defined to support separation standards. This importance becomes compounded in a mixed automation environment (e.g., with traditionally piloted aircraft in uncontrolled airspace) where the avoidance maneuvers between the conflicting aircraft become less explicitly coordinated.

## A.4 Fallback Capability Decomposition

Failure Identification and Annunciation: The ability of systems (human or machine) to identify failures during operations are crucial to ensuring safety in the airspace. As the capability of systems to identify nominal and off-nominal conditions expands, so too does the potential information that may be shared with the aircraft operator. The type, quality, and timeliness of this information are essential to ensure that humans can react effectively to changes in aircraft systems, components, and airspace services to manage operations (even if they aren't directly involved in the control or management of the aircraft). Further, this capability is essential to help inform contingency management and handover of system control as necessary.

Contingency Management: As part of flight planning, operators must plan for contingencies in the event of off-nominal flight conditions (e.g., aircraft system failures, airspace changes, emergency events). While in operation, an operator has to identify situations that will trigger contingency conditions (e.g., aircraft system failure, no-fly zone, vertiport closure, weather events) and respond appropriately along with other users in the operation airspace. Contingency management quickly becomes a complex systems problem with multiple aircraft, multiple contingencies, and multiple operators needing to de-conflict to manage an off-nominal situation. Automation of this capability helps manage that complexity. However, it creates opportunities for miscommunications, blunders, and unsafe operations if it is not carefully considered in the airspace system design (e.g., expected procedures, service infrastructure, and robustness/reliability requirements).

Safe Landing: Landing safely is the ultimate goal of any operation. In some cases, a safe landing may be off nominal (e.g., aircraft recovery systems, forced landing) but still acceptable. The determination of safe landing may be affected by the operating capabilities of an aircraft and its airspace environment. When an aircraft is in a degraded mode of operation, what was considered a safe landing during normal operations may change (e.g., declaring an emergency and landing immediately). This capability has tie-ins to contingency management, and an "emergency landing" may form a core contingency (depending on the operational risk). As landing systems continue to be automated (e.g., Garmin Auto-land), the impacts, both to nominal and off-nominal operations, need to be considered (e.g., a computerized emergency landing should not create a hazardous situation for other airspace users). Much like contingency management, flight rules, standardized procedures, and clear communication between airspace users will help reduce these risks as the level of automation rises.

Airspace Management: The final element involved in this capability is the control or management of other traffic in proximity to the automated aircraft operating in a fallback mode. Communication from the aircraft in the fallback mode of operation or the operator of that aircraft will allow the appropriate airspace control or management authority to clear the airspace or landing area or take other actions to facilitate contingency operations.

## A.5 Communication with External Systems (Ground and Airspace systems) Capability Decomposition

Air Traffic Management and Services (ATM/ATS): Air Traffic Services form a significant component of existing aviation operations (e.g., separation services, traffic information services). As UAS operations expand the variety of services offered will increase. Understanding the relationship between these services and the airspace structure, along with the dependency of services for particular air operations (including during contingencies and emergencies), helps inform the criticality of services. As the establishment and delivery of these services are automated, operations will likely become more efficient, but these services also provide a potential common source of error/failure. Challenges with the delivery of these services will range depending on: the equipage/service subscription requirements in a particular airspace, level of automation/capabilities of aircraft, and the traffic "mix" (traditional vs. UAS). Finally, Controller guidance (i.e., instructions from ATC to the pilot/aircraft) needs to be considered a particular case due to the current dependence on voice commands and responses. This special consideration is necessary due to the responsibilities of ATC to maintain aircraft separation in controlled airspace environments, and specifically between traditionally piloted, remotely piloted, and entirely autonomous aircraft. The requirements for all aircraft to understand and respond to ATC commands are crucial aspects of automating the airspace beyond its current capability. The level of automation of air traffic services in the airspace will be critical in the safe integration of automated operations. Automation of the airspace environment will be addressed in another JARUS document.

Sharing Intentions and Contingencies with other Airspace Users: Communication between airspace users is ubiquitous. From common radio frequencies, to equipment (left/right side lights), to physical maneuvers ("waggling the wings") communication, especially in congested airspaces, is essential to ensure the safety of the airspace. In addition, as communications systems advance, operators must look to share operational intents (e.g., flight plans) and contingencies (when triggered) with other airspace users (including Air Traffic Service Units). This is important for automated flight planning and managing operations in increasingly automated environments (evaluating conformance to flight intents). The communication of this information between operators is one of the significant informational pieces in ensuring efficient operations and that safe separation between aircraft is maintained.

Weather: In traditional aircraft operations, weather events are directly observable by the pilots on-board. With remote pilots, the detection of weather events becomes much more dependent on remote sensors (either onboard the aircraft or via a weather service, noting that the current model for weather reporting may be insufficient for automated operations). As changes in the weather environment occur, the operational limitations of the aircraft may change causing the aircraft to enter different flight (or control) regimes. As aircraft and airspace systems are automated, the effects that automated weather detection and reporting services have on operations in affected airspaces (especially micro-weather environments) need to be understood (e.g., adverse weather reporting triggering contingencies for less weather capable aircraft).

Example Template:

| Capability Dependency Matrix | Position Assurance | Common Navigation Reference | Flight Management and Operational Envelope Assurance | Dynamic Systems Coordination | Multiple System Management | Tolerable Latencies | Aircraft Control Handoff | System Status Awareness | Failure Identification and Annunciation | Contingency Management | Safe Landing | Geographic limit and Airspace awareness | Terrain and Obstacle Avoidance | Aircraft and Airborne Hazard Avoidance | Air Traffic Services communication and Control Guidance | Sharing Intentions and Contingencies with other Airspace Users | Weather |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Position Assurance | ■ | | | | | | | | | | | | | | | | |
| Common Navigation Reference | | ■ | | | | | | | | | | | | | | | |
| Flight Management and Operational Envelope Assurance | | | ■ | | | | | | | | | | | | | | |
| Dynamic Systems Coordination | | | | ■ | | | | | | | | | | | | | |
| Multiple System Management | | | | | ■ | | | | | | | | | | | | |
| Tolerable Latencies | | | | | | ■ | | | | | | | | | | | |
| Aircraft Control Handoff | | | | | | | ■ | | | | | | | | | | |
| System Status Awareness | | | | | | | | ■ | | | | | | | | | |
| Failure Identification and Annunciation | | | | | | | | | ■ | | | | | | | | |
| Contingency Management | | | | | | | | | | ■ | | | | | | | |
| Safe Landing | | | | | | | | | | | ■ | | | | | | |
| Geographic limit and Airspace awareness | | | | | | | | | | | | ■ | | | | | |
| Terrain and Obstacle Avoidance | | | | | | | | | | | | | ■ | | | | |
| Aircraft and Airborne Hazard Avoidance | | | | | | | | | | | | | | ■ | | | |
| Air Traffic Services communication and Control Guidance | | | | | | | | | | | | | | | ■ | | |
| Sharing Intentions and Contingencies with other Airspace Users | | | | | | | | | | | | | | | | ■ | |
| Weather | | | | | | | | | | | | | | | | | ■ |

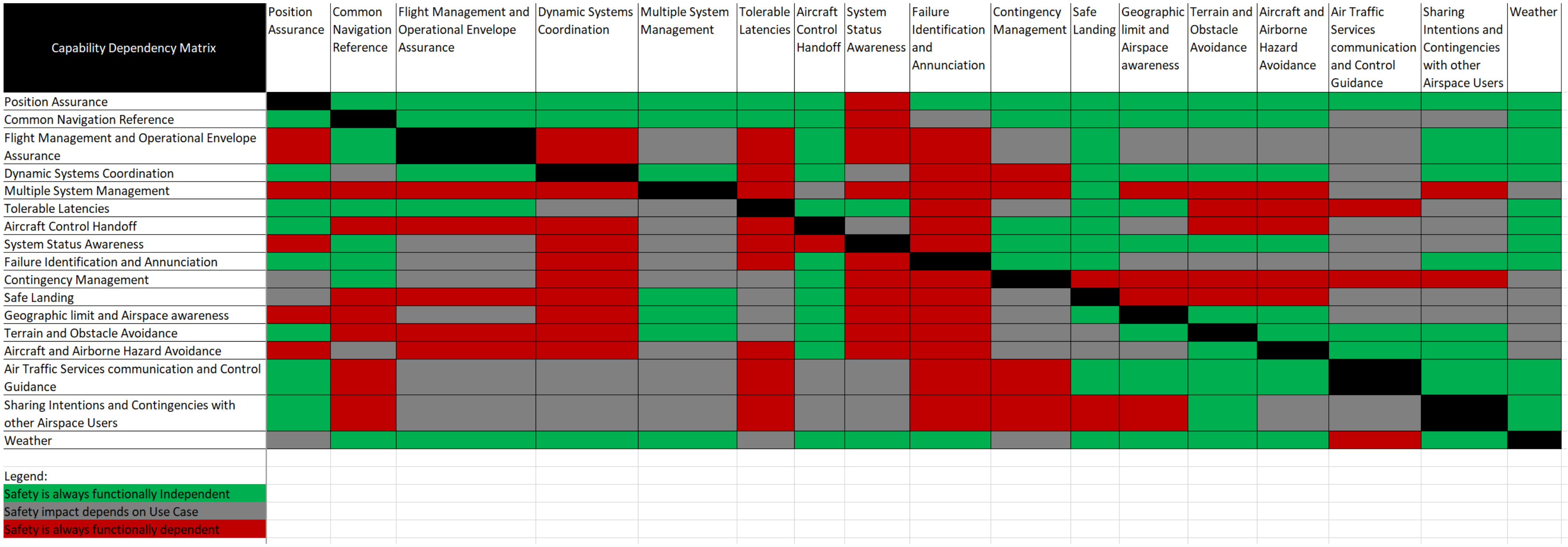
Legend:

🟥 Safety is always functionally Independent

⬛ Safety impact depends on Use Case

🟩 Safety is always functionally dependent

Example Evaluated Template (note: the table shows the dependence relationship of the column function to the row function, e.g., the Position Assurance function depends on the System Status Awareness function):



| Capability Dependency Matrix | Position Assurance | Common Navigation Reference | Flight Management and Operational Envelope Assurance | Dynamic Systems Coordination | Multiple System Management | Tolerable Latencies | Aircraft Control Handoff | System Status Awareness | Failure Identification and Annunciation | Contingency Management | Safe Landing | Geographic limit and Airspace awareness | Terrain and Obstacle Avoidance | Aircraft and Airborne Hazard Avoidance | Air Traffic Services communication and Control Guidance | Sharing Intentions and Contingencies with other Airspace Users | Weather |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Position Assurance | ⬛ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Common Navigation Reference | 🟩 | ⬛ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | ▨ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | ▨ | ▨ | 🟩 |
| Flight Management and Operational Envelope Assurance | 🟥 | 🟩 | ⬛ | 🟥 | ▨ | 🟥 | 🟩 | 🟥 | 🟥 | ▨ | 🟩 | ▨ | ▨ | ▨ | ▨ | 🟩 | 🟩 |
| Dynamic Systems Coordination | 🟩 | ▨ | 🟩 | ⬛ | 🟩 | 🟥 | 🟩 | ▨ | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | ▨ | 🟩 | 🟩 |
| Multiple System Management | 🟥 | 🟥 | 🟥 | 🟥 | ⬛ | 🟥 | ▨ | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟥 | 🟥 | ▨ | 🟥 | ▨ |
| Tolerable Latencies | 🟩 | 🟩 | 🟩 | ▨ | ▨ | ⬛ | 🟩 | 🟩 | 🟥 | ▨ | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | ▨ | 🟩 |
| Aircraft Control Handoff | 🟩 | 🟥 | 🟥 | 🟥 | ▨ | 🟥 | ⬛ | ▨ | 🟥 | 🟩 | 🟩 | ▨ | 🟥 | 🟥 | ▨ | ▨ | 🟩 |
| System Status Awareness | 🟥 | 🟩 | ▨ | 🟥 | ▨ | 🟥 | 🟥 | ⬛ | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | ▨ | ▨ | 🟩 |
| Failure Identification and Annunciation | 🟩 | 🟩 | ▨ | 🟥 | ▨ | 🟥 | 🟩 | 🟥 | ⬛ | 🟩 | 🟩 | ▨ | ▨ | ▨ | ▨ | 🟩 | 🟩 |
| Contingency Management | ▨ | 🟩 | ▨ | 🟥 | ▨ | ▨ | 🟩 | 🟥 | 🟥 | ⬛ | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | ▨ |
| Safe Landing | ▨ | 🟥 | 🟥 | 🟥 | 🟩 | ▨ | 🟩 | 🟥 | 🟥 | ▨ | ⬛ | 🟥 | 🟥 | 🟥 | ▨ | ▨ | ▨ |
| Geographic limit and Airspace awareness | 🟥 | 🟥 | ▨ | 🟥 | 🟩 | ▨ | 🟩 | 🟥 | 🟥 | ▨ | 🟩 | ⬛ | 🟩 | 🟩 | ▨ | ▨ | ▨ |
| Terrain and Obstacle Avoidance | 🟩 | 🟥 | 🟥 | 🟥 | 🟩 | ▨ | 🟩 | 🟥 | 🟥 | ▨ | ▨ | 🟩 | ⬛ | 🟩 | 🟩 | 🟩 | ▨ |
| Aircraft and Airborne Hazard Avoidance | 🟥 | ▨ | 🟥 | 🟥 | ▨ | 🟥 | 🟩 | 🟥 | 🟥 | ▨ | ▨ | ▨ | 🟩 | ⬛ | 🟩 | 🟩 | ▨ |
| Air Traffic Services communication and Control Guidance | 🟩 | 🟥 | ▨ | ▨ | ▨ | 🟥 | ▨ | ▨ | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | ⬛ | 🟩 | 🟩 |
| Sharing Intentions and Contingencies with other Airspace Users | 🟩 | 🟥 | ▨ | ▨ | ▨ | 🟥 | ▨ | ▨ | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | ▨ | ▨ | ⬛ | 🟩 |
| Weather | ▨ | 🟩 | 🟩 | 🟩 | 🟩 | ▨ | 🟩 | 🟩 | 🟩 | ▨ | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | ⬛ |

Legend:

🟩 Safety is always functionally Independent

▨ Safety impact depends on Use Case

🟥 Safety is always functionally dependent

# Appendix B – Automation Functional Impact Assessment

This appendix provides an example of how the functional automation of a particular UAS may be assessed using the impact assessment methodology described in this paper. This example utilizes the functional breakdown provided in Appendix A – ODD Functional Decomposition, but does not provide detailed assessments for every function of the UAS (as it is only meant as a demonstrative example). Additional guidance from national and international regulatory guidance and standards development organizations may be used to support and augment this assessment.

## B.1 Redundancy Determination

A UAS is composed of different systems, which performs several functions; each of them has a particular reason to be there. By analysing the purpose of each system or function, it can be differentiated into two main categories:

- **Safety-oriented:** Functions necessary to assure operational safety e.g., an autopilot to assure the flight envelope, GPS to assure the position.
- **Operational-oriented:** Functions to achieve the objectives of the flight, but not necessary to fly safely e.g., a camera for filming, objects for delivery.

Note that there could be some systems which could contribute to both functions, for example, a LiDAR could be used for mapping (operational-oriented) and at the same time be used to avoid obstacles (safety-oriented). In these cases, the safety-oriented function should take precedence.

The safety dependence is defined based on two attributes of a capability:

1. The available redundancy for carrying out the specific function, that is, if there are two or more different technological systems performing the functions; and
2. The operational contingencies are triggered in the case of a single failure of a system that performs the function, that is, if the function is degraded.

Taking into account these different alternatives, the following table describes the safety dependence of a function:

| | | Redundancy | |
|---|---|---|---|
| | | Yes | No |
| Operational limitation triggered | Yes | Partially safety dependent | Safety dependent |
| | No | Safety independent | Operational oriented |

## B.2 Equipment Architecture & Functional Impact

In the following table some examples of capabilities are analysed by describing the potential combinations of some available equipment for each safety dependency case:

| Capabilities | Safety independent | Partially safety dependent | Safety dependent |
|---|---|---|---|
| | **Redundant = Yes, Limitation = No** | **Redundant = Yes, Limitation = Yes** | **Redundant = No, Limitation = Yes** |
| Position Assurance | GPS + (GPS/GALILEO/GLONASS) + Independent Positioning System | GLONASS + GPS | RTK |
| Flight Management and Operational Envelope Assurance | Triple autopilot + 2 Management board | Double autopilot | Single autopilot |
| Tolerable Latencies (Spectrum optimization) | Independent redundant transceivers | Auto frequency selector | Power selector |
| Terrain and Obstacle Avoidance | Sonar + LiDAR | Double Sonar | Single Sonar |
| Aircraft and Airborne Hazard Avoidance | Multicamera EO (with 2 boards) + RADAR | Electro-Optical Sensor (EO) + RADAR | Single camera EO |

### Position Assurance

If a single GNSS receiver and single constellation is used, for example GPS on a single receiver, it is not redundant and it leads to an operational limitation in case of hardware failure, lack of sufficient line-of-sight satellites, or performance of the GPS constellation.  In this case, it is **safety dependent**.

If two different GNSS constellations on a receiver are used, like GPS+GLONASS, it is redundant, and if a constellation fails, the system can be positioned by using the other one, which could have lower accuracy or lower visibility, so it is **partially safety dependent**, but still limited to a HW failure of the receiver.

If two receivers of the same constellation (like GPS) are used, is redundant but it leads to an operational limitation in case of failure of the constellation (degradation to zero), so it is **partially safety dependent** as well.

There is no safety independent implementation of GNSS without additional independent positioning equipment which function within the defined operational limits.  Even if multiple constellations and receivers are used, satellite availability due to buildings and terrain can still limit the operation of the system.  Services like RTK can be safety dependent if it would cause abnormal performance of the UAS when lost.  RAIM and Geospatial Augmentation can be used to reduce the likelihood of GNSS degradation or failure and would be **safety dependent**.

Addition of an alternate independent positioning system that met at least the best-case accuracy of the GNSS systems would be **safety independent**.

## Aircraft and Airborne Hazard Avoidance

An electro-optical sensor system will detect aircraft and provide avoidance alerts, but if the meteorology conditions are lower than the minimum required or if the management board fails, it leads to an operational limitation, so it is **safety dependent**.

If a primary RADAR is used as a redundancy, the EO could fail in the same way as before, and the range of the RADAR could be lower, so it is **partially safety dependent**.

If a multicamera EO with redundant management board + a primary RADAR are used, there is no single failure possible that leads to an operational limitation, so it **is safety independent**.

## Flight Management and Operational Envelope Assurance

In a single autopilot, if anything fails, for example, the data provided from the inertial measurement unit, there is an operational limitation because of working with degraded data, so it is **safety dependent**.

When using two autopilots for redundancy, there should be a management board for comparing data, if data from each autopilot is different, there is a degradation because there is no way to know which autopilot is correct, so it is **partially safety dependent**.

If three autopilots are used, there should be a management board for comparing data and, if two autopilots provide the same data, there is no operational limitation because of the knowledge that is the other one the one that failed. If the single failure is in the management board, the output of which is the degraded autopilot could be wrong, so it could lead to an operational limitation, so it would be necessary to have three autopilot + two management boards to be **safety independent**.

## Equipment Architecture

If a single technology is used, the function will be safety dependent.

If two different technologies are used, depending on the possible failures, it could be partially safety dependent or safety independent.

There are technologies that could fail externally, like GNSS, which if a whole constellation stops working, the system that depends on the technology, stops working too. In all these cases, there are factors out of the scope of the operator that can lead to an operational limitation.

On the other hand, there are other technologies which do not depend on external factors, like using sonar for distance measurement or an anemometer for speed calculation. In these cases, having redundant system is enough because the operational limitation just can come from a failure in the own system, which is solved with redundant dissimilar technologies.

For this analysis, the safety dependency of a particular equipment architecture will be:

| *In General* | **Technology depending on external factors** | **Technology self-contained** |
|---|---|---|
| **Safety dependent**<br>(Redundancy=No, Limitation = Yes) | One system | One system |
| **Partially Safety dependent**<br>(Redundancy=Yes, Limitation = Yes) | Two systems (same or different tech) | Two same tech systems |
| **Safety Independent**<br>(Redundancy=Yes, Limitation = No) | Two different tech systems + one with self-contained technology | Two different tech systems |

An example of the Position Assurance function would look like:

| *Position Assurance* | **Technology depending on external factors** | **Technology self-contained** |
|---|---|---|
| **Safety dependent**<br>(Redundancy=No, Limitation = Yes) | GPS | Sonar |
| **Partially Safety dependent**<br>(Redundancy=Yes, Limitation = Yes) | GPS + GLONASS | Two sonar |
| **Safety Independent**<br>(Redundancy=Yes, Limitation = No) | GPS + GPS/GALILEO/GLONASS + Independent Positioning System<br>Or<br>Two GPS + INS | Sonar + LiDAR |

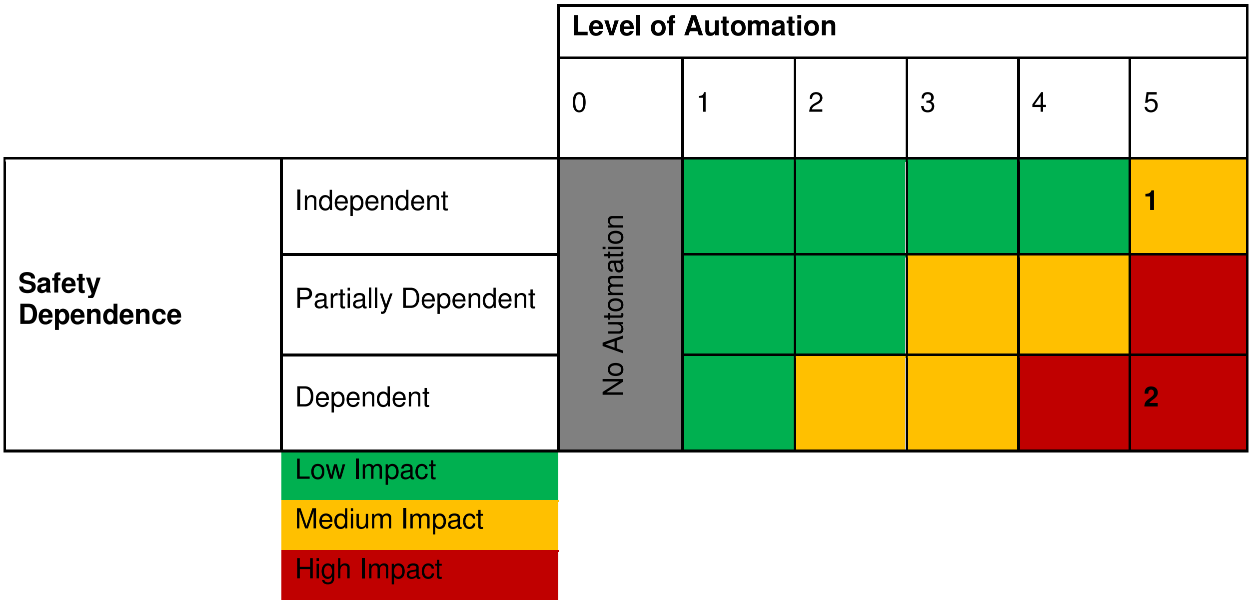
For an architecture with one self-contained technology and one technology which depends on external factors (instead of two self-contained systems like the safety independent cases) the analysis would lead to an assignment of partially safety independent.

## B.3 Automation Impact

After determining the functional architecture and technological dependencies the automated capabilities can be described via their safety dependence:

1. Flight Management and operational envelope assurance:
    - Three autopilot + two management boards are used for flight management and envelope assurance, so it is a **safety independent** function.
2. Terrain and Obstacle Avoidance:
    - A sonar is used, so it is a **safety dependent** function.

By using Table 2, the impact on safety of a capability depending on the level of automation (LoA) and the safety dependence can be evaluated.



| | | **Level of Automation** | | | | | |
|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 |
| **Safety Dependence** | Independent | No Automation | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 **1** |
| | Partially Dependent | | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 |
| | Dependent | | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 **2** |

🟩 Low Impact
🟨 Medium Impact
🟥 High Impact

We conclude with the following results:

1. Flight Management and operational envelope assurance
    - Medium impact

2. Terrain and Obstacle Avoidance
    - High impact

Using the same process, the automation impact to each capability described identified in Table B.2 above can be assessed. This impact would then need to be combined with the operational risk to determine the correct level of robustness to mitigate the risks to people in the air and on ground.

| Capability | Redundant? | Operational limitation in case of single failure? | LoA | Safety Dependence | Impact |
|---|---|---|---|---|---|
| Position Assurance | Yes | Yes | 5 | Partially | High |
| Flight Management and Operational Envelope Assurance | Yes | No | 5 | Independent | Medium |
| Tolerable Latencies (Spectrum optimization) | - | - | - | - | - |
| Terrain and Obstacle Avoidance | No | Yes | 5 | Dependent | High |
| Aircraft and Airborne Hazard Avoidance | Yes | No | 5 | Independent | Medium |

Further integration of the concepts in this document into other JARUS work products (e.g., SORA) is on-going.