World Academy of Science, Engineering and Technology
International Journal of Mechanical and Mechatronics Engineering
Vol:12, No:5, 2018

Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process

Achim Washington, Reece Clothier, Jose Silva

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

Abstract**—**System Safety Regulations (SSR) are a central component to the airworthiness certification of Unmanned Aircraft Systems (UAS). There is significant debate on the setting of appropriate SSR for UAS. Putting this debate aside, the challenge lies in how to apply the system safety process to UAS, which lacks the data and operational heritage of conventionally piloted aircraft. The limited knowledge and lack of operational data result in uncertainty in the system safety assessment of UAS. This uncertainty can lead to incorrect compliance findings and the potential certification and operation of UAS that do not meet minimum safety performance requirements. The existing system safety assessment and compliance processes, as used for conventional piloted aviation, do not adequately account for the uncertainty, limiting the suitability of its application to UAS. This paper discusses the challenges of undertaking system safety assessments for UAS and presents current and envisaged research towards addressing these challenges. It aims to highlight the main advantages associated with adopting a risk based framework to the System Safety Performance Requirement (SSPR) compliance process that is capable of taking the uncertainty associated with each of the outputs of the system safety assessment process into consideration. Based on this study, it is made clear that developing a framework tailored to UAS, would allow for a more rational, transparent and systematic approach to decision making. This would reduce the need for conservative assumptions and take the risk posed by each UAS into consideration while determining its state of compliance to the SSR.

Keywords**—**Part 1309 regulations, unmanned aircraft systems, system safety, uncertainty.

I. Introduction

THE UAS industry is the fastest growing sector of the commercial aviation industry. However, the integration of UAS into the ultra-safe aviation sector poses some challenges. All technologies have associated safety risks. Currently, the majority of UAS do not exhibit the same high reliability shown by conventionally piloted aircraft. A recent study conducted by the Australian Transport Safety Bureau (ATSB) showed that the number of reported Remotely Piloted Aircraft Systems (RPAS) occurrences between January 2012 and December 2016 was approximately 180. The models used to forecast the number of reported occurrences also saw a 60% increase in this number in 2017 when compared with 2016 [1]. To date, the safety risks associated with civil/commercial UAS operations are largely managed through restrictions on their operation [2]. These restrictions include prohibiting their flight over populated regions or in close proximity to people. This can impede the utility of UAS in a wide range of civil and commercial applications.

The risks presented to people and property overflown can be managed through the implementation of a range of technical and operational risk controls [3]. One such control is ensuring a higher degree of airworthiness, and in turn reliability, in the operated system. Airworthiness can be defined as, "the condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function" [4]. The item (aircraft, aircraft system, or part) is defined as airworthy if it is certified against the appropriate set of airworthiness regulations. For example, STANAG 4671 establishes the baseline set of airworthiness standards in relation to the design and construction of military UAS [5].

It is now broadly recognised that airworthiness regulations should be tailored to the different UAS types and their Concepts of Operations (CONOPs), and that this tailoring should be governed by the level of risk posed. Further, not all UAS types may be required to meet prescriptive codes of airworthiness requirements in order to be safe for operation. EASA has proposed a risk-based airworthiness regulatory framework that divides airworthiness of UAS into the three categories of: 1) Open, 2) Specific, and 3) Certified [6]. UAS in the Specific and Certified categories are likely to require certification against prescriptive codes of airworthiness requirements (or parts of). These requirements are likely to include compliance to SSR, also referred to as "Part 1309 regulations".

Compliance with the SSR is a central component to the airworthiness of any aviation system. SSR supplement prescriptive requirements on the design and testing of an aviation system and are, in part, put in place "to ensure that an aircraft is capable of continued safe flight and landing following a failure or multiple failures of systems" [7]. The regulations can be applied to installed sub-systems or an aircraft system as a whole. SSR are briefly discussed in Section II.

There is ongoing debate on the setting of appropriate SSR for UAS [8]. Putting this debate aside, the next challenge lies

Achim Washington is a PhD candidate at the School of Engineering, RMIT University, Melbourne, Australia (corresponding author, e-mail: s3270338@student.rmit.edu.au).

Reece Clothier is a Principal Researcher at Boeing Research & Technology- Australia and Adjunct Associate Professor at RMIT University, Melbourne, Australia (e-mail: reece.a.clothier@boeing.com).

Jose Silva is a Senior Lecturer with the School of Engineering, RMIT University, Melbourne, Australia (e-mail: jose.silva@rmit.edu.au).

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

in how to apply the system safety assessment and compliance process to UAS. These challenges are discussed further in Section III. Addressing these challenges is critical to the eventual airworthiness certification of UAS, and subsequently, to enabling UAS operations in increasing populous areas.

There is continuing research into addressing these challenges [9], [10]. This research has focused on how to better account for uncertainty in the System Safety Assessment (SSA) process (as currently used for conventional civil aviation systems) and how to improve compliance findings and decision making in the presence of uncertainty. The revised system safety process described in [9], [10], enables a fundamentally new approach to regulatory decision making, that of making compliance decisions on the basis of risk. The process is particularly suited to UAS and any other aviation system or sub-system where there is limited knowledge and data to base assessments of safety performance.

Section III of this paper summarises the broader research endeavour of existing research [9], [10] and future research. The advantages of these modified frameworks, and application to the SSA of civil/commercial UAS are also described in Section IV.B. The limitations of current research and avenues for extension are presented in Section III.C, with concluding remarks outlined in Section IV.

II. System Safety Regulations (SSR)

SSR are contained in sub-part 1309 of conventionally piloted aircraft airworthiness certification regulations (e.g. CS/FAR 23.1309 [11] for aeroplanes in the normal, utility, acrobatic or commuter category and CS/FAR 25.1309 [12] for aeroplanes in the transport category). They supplement prescriptive standards on the design, manufacture, and installation of aircraft components, and at a high level, specify the requirements for [13]:

- A documented analysis showing that equipment and systems perform as intended under foreseeable operating and environmental conditions;
- The adoption of principles from fail-safe and fault-tolerant design [12]; and
- The demonstration (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system.

The latter requirement is commonly referred to as the SSPR and is the particular element of SSR that this research is focused on.

The SSPR establishes a minimum acceptable level of reliability of aviation equipment and components. It comprises of three sub-processes, namely the SSA, Compliance Assessment (CA), and Compliance Finding (CF) sub-processes [9]. The sub-processes and the interactions between them are illustrated in Fig. 1 and are discussed further in the following three sub-sections. The limitations of the overall SSPR compliance process are outlined in Subsection II.D.

A. System Safety Assessment Process

The purpose of the SSA process is to identify potential system failures and their safety effect, determine the likelihood of their occurrence, and assign a relevant safety objective. Inputs to the SSA process include component reliability data, expert knowledge, concept of operations, and system baseline description.

The SSA process includes a number of sub-processes that can be applied at different stages of a product lifecycle. Detailed in the SAE ARP 4761 are a range of recommended supporting tools and techniques that can be used within the process, including Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), Common Mode Analysis (CMA), etc. [4]. Further details on the SSA process and the tools used in a SSA can be found in [4], [9], [14].

Outputs from the SSA process include:

- a description of identified failure conditions,
- associated assessments of the failure severity category,
- associated assessments of the average probability of failure per flight hour (APFH) of the failure conditions being realised, and
- an assignment of applicable failure probability objective (FPO).

These outputs can be represented by the four sets *F, C, Λ* and *O*, respectively (1)-(4).

$$F = \{f_n : n \in Q\} \quad (1)$$

$$C = \{c_n : n \in Q\} \quad (2)$$

$$\Lambda = \{\lambda_n : n \in Q\} \quad (3)$$

$$O = \{o_n : n \in Q\} \quad (4)$$

The integer set *Q*, given in (5), is used to index an assessment for a specific failure condition (f_n), where *N* corresponds to the total number of unique failure conditions identified within the SSA process. The output assessment for a specific failure condition (f_n) is described by the tuple given in (6).

$$Q = \{n | n \in \mathbb{Z}^+, n \leq N\} \quad (5)$$

$$< f_n, c_n, \lambda_n, o_n > \qquad where \;\; n \in Q; \quad (6)$$

System safety advisory materials (e.g., [11], [12]) define the qualitative and quantitative scales to be used for the assessment of the failure severity category and APFH. An example of these scales, based on those provided in airworthiness regulations for UAS [7] and manned systems [11], are provided in Tables I-III in the Appendix. The FPO is qualitatively described in the SSR and depends on the particular certification category of the aircraft or component. It is often represented graphically as shown in Fig. 8 of the Appendix.

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

B. Compliance Assessment Process

CA can be thought of as a process of determining the degree to which a candidate system meets relevant requirements. Inputs to the CA process are the *N* tuples described in (6). For each assessment, a simple deterministic binary "pass or fail" process is applied, whereby, λ_n (the APFH assessed for a specific failure condition f_n) is compared to its corresponding FPO (o_n) to determine the state of compliance. The state of compliance for the n^{th} identified failure mode, h_n, is true if λ_n is less than o_n, as given in (7):

$$h_n = \begin{cases} True & if\ |\lambda_n| \leq o_n \\ False & otherwise \end{cases} \tag{7}$$

The CA process is undertaken for all *N* assessed failure conditions, with the resulting compliance state assessments contained in the set *H*.

$$H = \{h_n :\ n \in Q\} \tag{8}$$

An overall compliance state of the system, H_S, is determined as *True* if it can be shown that all the assessed APFH satisfy their FPOs (*i.e.*, all h_n are *True*), (9).

$$H_s = \begin{cases} True & if\ h_n = True\ \forall_n \in Q \\ False & otherwise \end{cases} \tag{9}$$

C. Compliance Finding Process

The CF process is a simple deterministic decision-making process. The system is deemed compliant to the Part 1309 SSPR if the following conditions hold:

- H_s is *True*; and
- All necessary documentation on the assessment outcomes, people, tools, and data used as part of the SSA and compliance processes is provided.

If the system is determined to be non-compliant (*i.e.*, H_s = *False*) then an iterative engineering process is usually undertaken to reduce the APFH and/or the failure condition severity, as shown by the dotted line in Fig. 1. It is possible for regulators to declare a system as non-compliant based on insufficient evidence of compliance. In such cases, further information or a reassessment is required (shown as a feedback path in Fig. 1). A system is then deemed as compliant (or not) with the SSPR, with the outcome forming part of its case for certification.

D. Limitation of Current SSPR Compliance Process

The SSA process can be conducted at the component, sub-system, or system level. Each assessment results in a set of outputs described by the tuple defined in (6). These assessments are however conducted independently of each other. Therefore, the interactions and dependencies between these components or sub-systems are not taken into consideration. While the current approach is simple and easy to implement, such dependencies would need to be taken into consideration in order to address the complexity of the overall problem and move towards a risk based approach to regulations.

Another major limiting assumption of the current SSA process is that it assumes a constant failure rate when providing an estimate of the APFH of the system. This essentially implies that the system is a mature system and as such is in the useful life phase of its operational life cycle, which is characterised by a constant failure rate. For new systems like UAS, owing to a number of factors described in the following section, the failure rate is not constant. The inability of the current SSA approach to take the reducing or increasing failure rate of the UAS into consideration is another limiting factor of the approach.

While the current SSPR compliance process does recognise that multiple failure scenarios are possible, it takes the worst-case scenario into account [14], thus failing to take the uncertainty associated with the other scenarios into consideration.

Uncertainty is inherent in every stage of the SSPR compliance process illustrated in Fig. 1. However, the current process does not comprehensively capture this uncertainty. Uncertainty manifests as uncertainty in the SSA process outputs, specifically:

1. *F* – Uncertainty in relation to whether all failure conditions have been identified (completeness), and whether each identified failure condition (f_n), is correctly specified in terms of its modes of failure and potential effects;
2. C – Uncertainty in relation to the estimate of the magnitude of consequential effects and in turn, the severity condition category (c_n) assigned to each of the identified failure conditions in *F*;
3. *Λ* – Uncertainty in relation to the estimate of the APFH (λ_n) for each failure condition;
4. *O* – Whether the correct FPO (o_n) is assigned to each identified failure condition.

The CA decision process described in (9) has no means for accounting for these uncertainties, with the CA output being a binary comparison with two possible outcomes: *True* or *False*. There is no objective means of expressing the resulting uncertainty in the output state of compliance. Consequently, decision makers are unable to objectively account for uncertainty when making compliance findings.

The uncertainty in the SSA process and CA process carries forward to the CF process. Its inescapable existence gives rise to six possible outcomes from the compliance decision making process as described in [9]. These range from certifying a UAS as compliant when it is in fact compliant (desirable outcome) to requiring further data and analysis when the UAS is in fact non-compliant (less than desirable outcome). There is currently no objective and mathematical means for a decision maker to decide between these outcomes. Decision makers use a subjective and somewhat "black box" process to make compliance findings and as such the process lacks the transparency and objectivity required of regulatory decision making.

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

III. Challenges in the Application of the SSPR Process to UAS

There are numerous on-going efforts to define suitable SSR for UAS. These include those specified by NATO [5], [15], EASA [16] and EUROCONTROL [17]. There are various points of contention between specifications [8]. Whilst the focus of this debate has been on the specification of the SSR, there has been limited research to date exploring the challenges associated with the application of the traditional SSPR compliance process to UAS; specifically, how to show compliance with the SSR.

UAS are fundamentally different from conventionally piloted aircraft (CPA), not only in the nature of their physical systems and how they are operated but also in the underlying philosophy and engineering processes used in their design and manufacture. These differences lead to unique challenges when it comes to their airworthiness certification. Some of the challenges described in [18], [19] include:

- Challenge associated with the regulatory surveillance enforcement;
- Accounting for the human system interaction in the assessment process;
- Need to certify the UAS based on both the function of the system and properties of the intended operational environment as opposed to just certifying the CPA based on the intended function of the system.
- Need to account for mitigation measures as part of the safety case when certifying the UAS as opposed to looking at the mitigation measures on a case by case basis when evaluating a CPA.

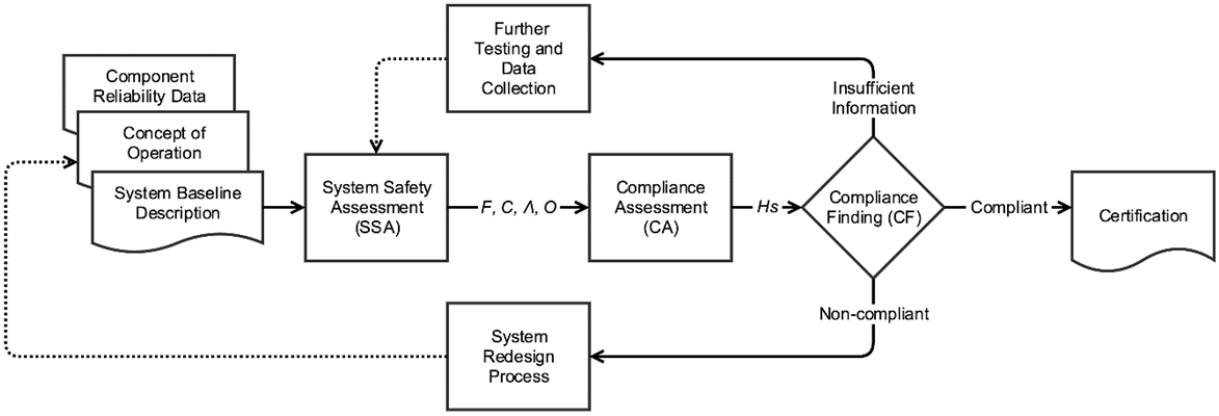

Fig. 1 Overview of the SSPR Compliance Process [9]

Further to the general challenges described in [18], [19], there are a number of important differences between UAS and CPA that can impact their certification:

- **Design philosophy** – many UAS have a different design trade space than CPA. For many UAS, system reliability can be determined by a trade-off between capability, cost, and restrictions on their operation. For manned aircraft, there is always a hard limit to this trade, dictated by the minimum reliability and system performance required to ensure the safety of those on-board. Some of the main issues in adopting new technologies such as UAS that impact this trade space are described in [20].
- **Engineering processes** – currently, many civil/commercial UAS are designed and manufactured in non-traditional aviation engineering environments. Many small UAS are designed by hobbyist, modelling and remote control flying enthusiasts. As a consequence, many UAS lack the supporting documentation, and systems engineering rigour that would be expected in the engineering of a CPA. This body of evidence is a key input to the SSPR process.
- **Technology refresh rate** – UAS types are rapidly evolving. A study conducted in [21] shows how technologies that are central to UAS have improved at a rapid pace over the years. This is driven by the need to 1) keep pace with new capability in component technologies (*e.g.*, new battery, sensing, autopilot, and communications sub-systems), 2) meet new and emerging requirements of new customers, and 3) to ensure that their product-offering is at the forefront of current capability. The high refresh rate coupled with the use of Commercial Off the Shelf (COTS) components makes it difficult to collect reliability data on systems and components.
- **Changing certification baseline** – Many UAS lack a static design baseline against which a certification case can be established. This stems from the high technology refresh rate and the customer demand for flexible and reconfigurable systems capable of performing a variety of missions. As a consequence, it can be difficult to develop significant safety heritage in a particular system configuration. In contrast, CPA have a relatively static system baseline. This allows safety data to be gathered for a single aircraft type or across the entire fleet of a particular aircraft type.
- **Unassured components** – UAS make extensive use of COTS components. COTS components are generally not designed, manufactured, or tested to an approved standard and therefore lack the necessary assurance of normal aviation components. These standards are an important input to the SSA process.

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

- **Lack of knowledge** – In general there is a lack of domain expertise in the design and operation of civil/commercial UAS when compared to CPA. This is owing to the relative infancy of the sector and restrictions on their operation. Expert judgment in relation to UAS design and operations is a key input to the SSA process. The lack of knowledge gives rise to uncertainty in the SSA process. This uncertainty can be in relation to known parameters or even unknown parameters (parameters that can impact the model but have not been taken into consideration owing to the lack of information available on them). Currently there is no means of representing this knowledge uncertainty in the SSA process.
- **Heterogeneity of fleet and operations** – There is significant diversity in the types, configurations, performance, and operational profiles of civil/commercial UAS. A study conducted in [19] shows that the Maximum Take-Off Weight (MTOW) of the UAS fleet ranged from a few grams to hundreds of tonnes, whereas for the CPA fleet, the MTOW ranged from a few hundred kilograms through to thousands of tonnes. Similarly, as can be seen from Fig. 2, there is significant diversity in the type of operations of the UAS as well. The heterogeneity of the UAS fleet and their operations makes it difficult to base assessments and develop knowledge through comparison.

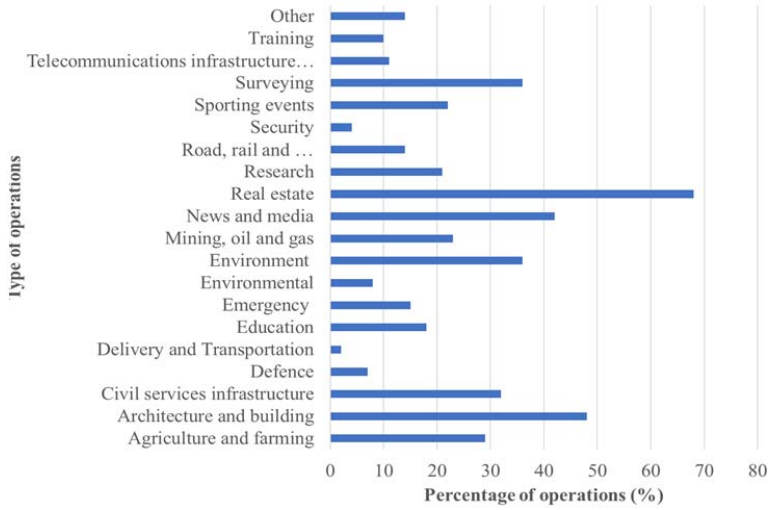

Fig. 2 Diversity in types of UAS operations, based on [22]

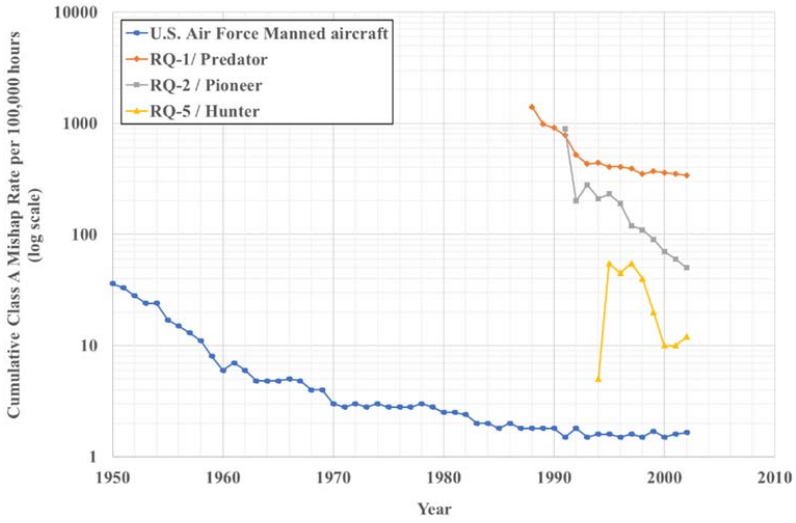

Fig. 3 Comparison of cumulative mishap rate based on [23]

- **Changing failure rate-** The current SSPR compliance process assumes a constant failure rate as CPA are mature systems that are in the useful life phase of their life-cycle. This assumption cannot be made for UAS as these systems are still relatively new and are in the infant mortality phase of their life-cycle. Factors like the design philosophy, technology refresh rate, use of COTS all contribute to systems with a dynamic baseline. Thus, the failure rate of many systems might never reach a stable/constant value. An example of the mishap rate for

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

UAS compared to manned systems based on [23] is shown in Fig. 3. From this, it can be seen that the mishap rate of the UAS has still not reached a constant value, while that for manned aircraft has become relatively stable. The limited data available on UAS compared to manned aircraft can also be seen here.

As a result of these differences, there is a general lack of knowledge and operational data, and a lack of trust in the data and knowledge that is available, to support airworthiness assessment and compliance finding processes for UAS. There can be considerable uncertainty associated with the certification of civil/commercial UAS, which in turn can lead to high certification risk (i.e., the risk associated with certifying a UAS as compliant, and therefore safe for operation, when indeed it is not).

The SSPR compliance process as used for the certification of CPA does not adequately account for the high uncertainty inherent to the SSA of UAS. System safety guidance materials [4], [11], [12], [14], [24] make no explicit mention of uncertainty, its measurement or treatment as part of a SSA. Reference [14] acknowledges that a failure mode can potentially have a range of negative impacts on the safety of flight. In such cases, the recommended practice is to assign the highest potential severity category c_n. In so doing, uncertainty in the set of potential consequential outcomes is discarded and can result in an overly conservative failure probability objective being assigned to the system. While this may not adversely impact the safety of the general public, it does result in the imposition of unnecessarily stringent restrictions on the design of UAS. This in turn comes at the cost of capability and system cost.

The reliability of a UAS can be improved in a number of ways including, investing in more advanced and expensive components that have been designed to higher standards and installation of redundant systems to use in case of emergencies. While it is important to have a UAS with components that are designed to a certain level of reliability and with redundant systems put in place, this needs to be balanced with the cost (both in terms of monetary costs and costs in terms of added weight, volume and power consumption to the system) involved in installing these components and the risk posed by having systems with lower reliability. The added components would result in a reduced payload capacity, range and endurance, thus limiting the potential applications.

Taking all of this into consideration, it is clear that research needs to be conducted into improving the current SSPR compliance process so that it is capable of taking the unique characteristics associated with UAS into consideration.

IV. Improving the SSPR Compliance Process

A new approach to regulatory compliance is to consider it as a problem of decision making under uncertainty. Jaynes [25] describes the desiderata of rationality and consistency for plausible reasoning in the presence of uncertainty. Based on this, decision makers can only make inferences (or propositions) about the state of the world based on the uncertain knowledge and information at hand. Bayesian inference provides a means for measuring uncertainty in relation to these hypotheses by producing information based on models, data, and other information [26]. In addition to this, Bayesian inference also allows for the state of knowledge (degree of belief in the hypothesis) to be progressively updated as new data or experience in the operation of the system is gained. Decisions are made on the basis of objective measures of uncertainty (or by extension, measures of risk) as opposed to binary statements of compliance. This approach to safety compliance has been explored for autonomous ships [27] and for showing assurance in autonomous UAS performance [28]. Within a safety assessment context, Bayesian approaches have been extensively used in the probabilistic risk assessment of space launch activities [29], [30] and nuclear power generation [31]. Such assessments are characterised as complex and based on sparse data; characteristics common to the SSA of UAS.

A. Extended SSPR Compliance Process

References [9] and [10] have begun to apply this general approach to the SSPR compliance process for UAS. The research to date has focused on addressing only the uncertainty in relation to the assessment of the APFH for individual failure conditions. The modified approach is illustrated in Fig. 6 and briefly described in this section. For further details the reader is directed to [9].

The principle modification lies in the SSA process, specifically, the quantification of the APFH. As described in Section II, the output set Λ contains point value assessments of λ_n of the APFH for each failure. This is depicted graphically in Fig. 4. Under the extended approach of [9], Bayesian methods are used to characterise the state of knowledge in each assessment of APFH as opposed to the value of λ_n. The modified output from the SSA process is the set Λ^*, which comprises N conditional probability distributions describing the uncertainty (or degree of belief) in λ_n. The probability distributions obtained replace the point-value assessments of the APFH originally output from the SSA process, as illustrated in Fig. 5. Each probability distribution, denoted by $p(\lambda_n|D,I)$ and given in (10) represents the state of knowledge in APFH for the given failure condition, where D represents data and I the knowledge and information available.

$$\Lambda^* = \{p(\lambda_n|D,I) : n \in Q\} \tag{10}$$

As shown in Fig. 6, these distributions are input to the CA process. Various inference approaches (hypothesis testing and Bayesian prediction) can be used to provide a measure of the uncertainty in the state of compliance with the FPO. The simple deterministic *True* or *False* output of the CA process is replaced by measures describing the degree of certainty in the state of compliance (*i.e.*, system failure meets its assigned FPO, o_n). Referring to Fig. 5, this can be visualised as the area under the curve that resides in the "acceptable" region.

As shown in Fig. 6, the CA uncertainty measures are then input to the CF process, which, in [9], has been structured as a simple normative decision-making problem. Whilst many

possible decision making formulations could be adopted, the normative approach ensures an objective, transparent, and systematic input to decision making. From [9], there are six possible outcomes from the CF process:

- The UAS is deemed to be compliant when it is actually compliant;
- The UAS is deemed to be compliant but it is actually non-compliant;
- The UAS is deemed to be non-compliant but it is actually compliant;
- The UAS is deemed to be non-compliant when it is actually non-compliant;
- There is insufficient information in the state of compliance when the UAS is actually compliant;
- There is insufficient information in the state of compliance when the UAS is actually non-compliant.

A loss/benefit function can be assigned to each possible outcome and combined with the uncertainty measures to provide measures of the compliance risk. A range of objective decision utility functions can then be applied to aid the regulator in making the best compliance decision (Reference [9] applied a simple minimum-risk decision selection function).

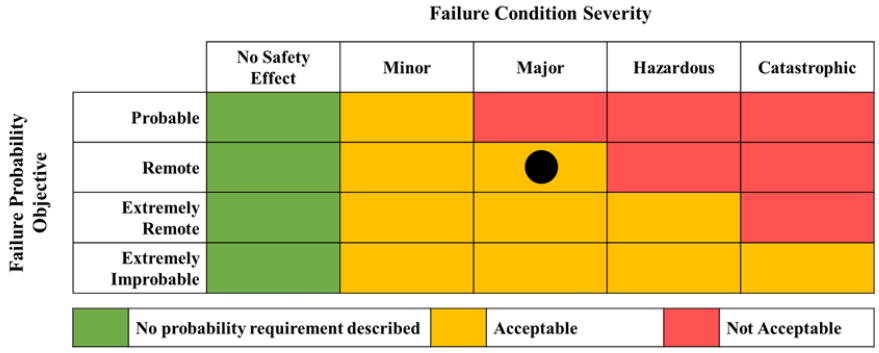

Fig. 4 Output from traditional SSA approach

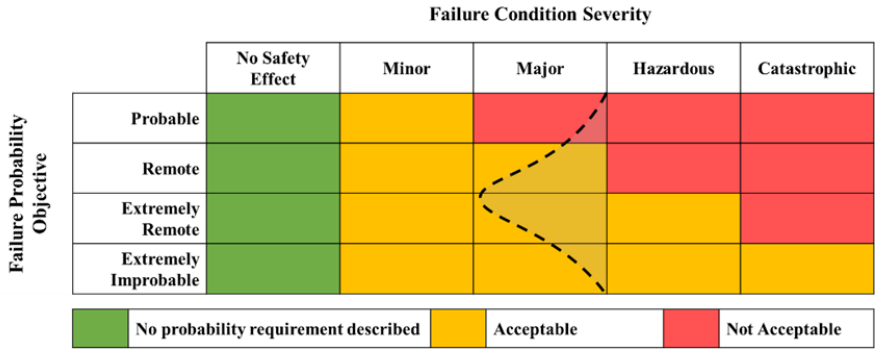

Fig. 5 Output from extended SSA approach

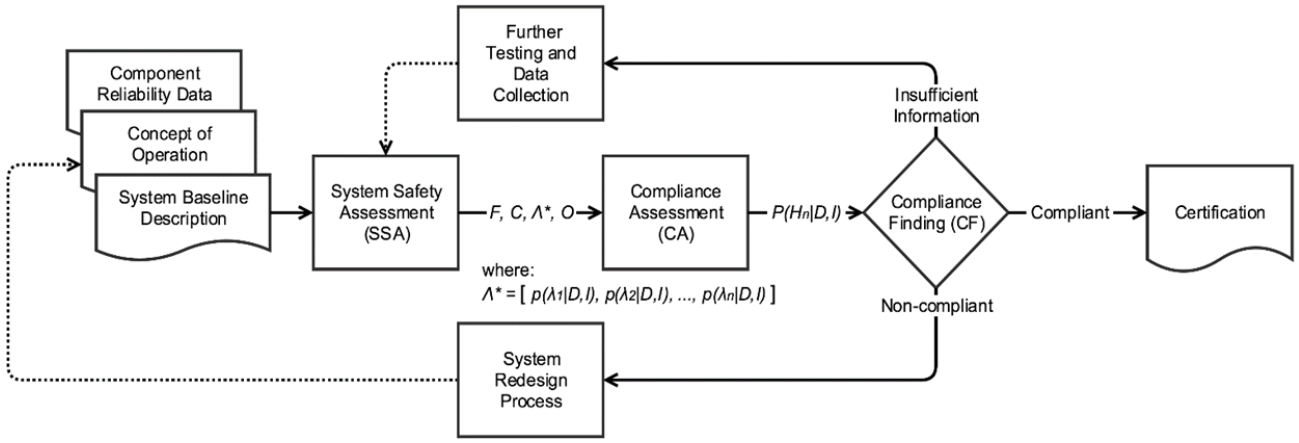

Fig. 6 Overview of the extended SSPR Compliance Process [9]

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

B. General Advantages

The approach provides a more transparent, rational, and systematic compliance decision-making process. It proposes a significant change to how aviation safety practitioners currently undertake regulatory compliance activities. The application of such an approach provides a:

- more comprehensive means for assessing and treating uncertainties inherent to the SSA of an aviation system;
- mathematically robust means for combining data with expert judgement in safety assessments;
- means to support inductive and deductive reasoning in relation to the system safety of UAS (e.g., predictive assessments or incident analysis);
- framework that is compatible with existing system safety modelling and analysis tools (e.g., Functional Hazard Assessments (FHA), Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), etc.);
- mathematically robust means for updating the state of knowledge as new data or operational experience is gained (a useful feature for rapidly evolving systems such as UAS);
- framework that supports more justifiable and systematic compliance findings;
- method for making airworthiness compliance decisions based on compliance risk;
- means for ensuring more transparent, objective, and consistent compliance findings in the presence of uncertainty; and
- means to reduce the need for conservative assumptions and the subsequent impost of unnecessary costs on the UAS industry.

C. Further Evolutions of the SSPR Compliance Process

The revised SSPR compliance process represents a paradigm shift in regulatory compliance. However, there remain a number of opportunities to further enhance the process to take better account of the issues identified in Section III.

The traditional SSA process assumes that failures occur at a constant rate. The same assumption was made in the approach developed in [9] through the use of a Poisson likelihood distribution. The assumption of a constant failure rate fails to account for the variable failure rate characteristic of most new systems like UAS (as described in Section III). The model presented in [10] addresses this shortcoming by adopting a Weibull distribution as the likelihood distribution.

There is also a need to extend the SSPR process to account for the uncertainty in the remaining outputs of the SSA process. For example, a single failure can have more than one failure mode, and in turn, different consequential effects. The uncertainty in relation to these different scenarios can also differ. This in turn can lead to uncertainty in the assignment of the correct FPO. This uncertainty has traditionally been addressed through the assignment of the worst case consequential outcome, which, as described previously, can lead to overly conservative requirements on the reliability of the system. This is a consequence driven as opposed to a risk driven regulatory approach. A means for capturing and representing all potential consequential outcomes (and in turn risk) associated with potential failure conditions is needed. The output for a single failure condition would thus be a set of assessments, conceptually shown in Fig. 7.

SSA processes make use of a wide range of data sources. From component reliability test data, incident, and accident reports, through to expert judgment based on operational experience or technical knowledge. Data uncertainty has yet to be fully accounted for in the current SSA approach. Current SSA guidelines recommend the use of sensitivity analysis, which does not account for biases, missing, or erroneous data. There are various techniques for accounting for input data uncertainty within a Bayesian context, which could be adopted and applied to the specific problem of UAS failure modelling.

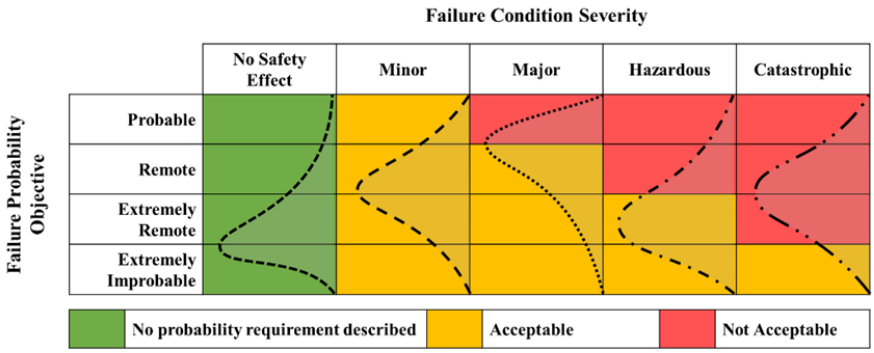

Fig. 7 Desired output from SSA approach

The current SSPR framework assumes independence in failure conditions and their management. This is largely necessitated by the need to manage complexity. The FPOs are derived from an apportionment of a system-level acceptable failure rate to individual failure conditions. Implicit to this apportioning is the assumption of independence. Common mode failures are considered in current SSA processes, however, the combined assessment and management of all failure conditions accounting for the dependencies between them, is not undertaken at the system level. Consequently, there is no guarantee the overall system-level safety objective is met.

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

More advanced modelling approaches are required to address these challenges. One such approach is through the use of Bayesian Belief Networks (BBN), which are particularly suited to higher level system modelling. Examples of the application of BBN to aviation operational risk modelling include [32]−[34]. These techniques have yet to be applied within the framework of a formal SSA within the SSPR compliance process.

V. Conclusion

System safety is a critical component of the airworthiness certification of UAS. Assurance in the airworthiness of UAS is needed to enable greater freedom of their operation in non-segregated airspace and over increasingly populous areas. Whilst research to date has focused on the specification of the SSR for UAS, there has been little effort directed towards understanding the suitability of existing regulatory compliance processes.

This paper has highlighted a number of challenges to the application of existing system safety compliance process to UAS. It is found that a more comprehensive treatment of the uncertainties inherent to the SSA of UAS is needed. Potential approaches for achieving this are presented.

UAS are revolutionising all aspects of aviation – the introduction of new technology, autonomy, operations, and airspace design and manufacturing processes. This evolution extends to the fundamental philosophy and approach to the safety regulation of aviation. Through UAS, there is the opportunity to reassess and evolve longstanding regulatory practices; potentially bringing them in line with more contemporary principles for safety management and decision making. An example of this is the move towards risk-based regulation for the UAS sector, a regulatory development principle that has equal applicability to all aviation sectors. With this in mind, the fundamental theory, process, and techniques explored within this paper have broader applicability to the aviation sector.

Appendix

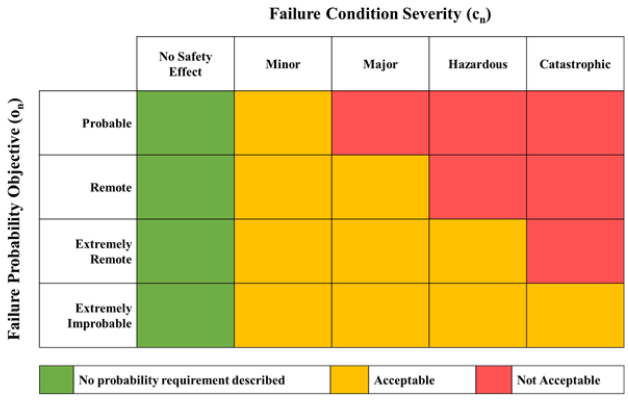

Fig. 8 Risk matrix showing FPO based on [7]

TABLE I
Qualitative Description of Failure Severity Categories for UAS Based on [7]

No Safety Effect
Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase remote crew workload.
Minor
Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.
Major
Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.
Hazardous
Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following; • Loss of the RPA [Remotely Piloted Aircraft] where it can be reasonably expected that a fatality will not occur, or • A large reduction in safety margins or functional capabilities, or • High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.
Catastrophic
Failure conditions that could result in one or more fatalities

TABLE II
Qualitative Description of Failure Probability Objectives for Manned Aircraft [11]

Probable
Those failure conditions anticipated to occur one or more times during the entire operational life of each airplane. These failure conditions may be determined on the basis of past service experience with similar components in comparable airplane applications.
Remote
Those failure conditions that are unlikely to occur to each airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type.
Extremely Remote
Those failure conditions not anticipated to occur to each airplane during its total life, but which may occur a few times when considering the total operational life of all airplanes of this type.
Extremely Improbable
For commuter category airplanes, those failure conditions so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type. For other classes of airplanes, the likelihood of occurrence may be greater.

TABLE III
Quantitative Description of FPO for UAS[1] [7]

FPO	Quantitative value (APFH)
Probable	$< 10^{-3}$ hr^{-1}
Remote	$< 10^{-4}$ hr^{-1}
Extremely Remote	$< 10^{-5}$ hr^{-1}
Extremely Improbable	$< 10^{-6}$ hr^{-1}

Acknowledgment

This research was supported, in part by, the Australian Government Research Training Program Scholarship, provided by the Australian Government.

[1] FPO described using Average Probability per Flight Hour

Open Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

REFERENCES

[1] ATSB, "A safety analysis of remotely piloted aircraft systems," 2017.
[2] CAA, "CAP-722, Unmanned Aircraft System Operations in UK Airspace - Guidance," London UK Civil Aviation Authority (CAA), Department of Transport (DfT), London, UK, 2015.
[3] R. A. Clothier, B. P. Williams, and K. J. Hayhurst, "Modelling the Risks Remotely Piloted Aircraft Pose to People on the Ground," *Saf. Sci.*, vol. 101, pp. 33–47, 2018.
[4] SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment." SAE International, 1996.
[5] NATO Standardization Agency (NSA), "STANAG 4671 - Unmanned Aerial Vehicles Systems Airworthiness Requirments (USAR)," Brussels, Belgium, 2009.
[6] EASA, "'Prototype' Commission Regulation on Unmanned Aircraft Operations - Explanatory Note," 2016.
[7] JARUS Working Group 6, "Safety Assessment of Remotely Piloted Aircraft Systems," *AMC RPAS.1309*, no. 2, 2015.
[8] EUROCAE, "UAS / RPAS Airworthiness Certification '1309' System Safety Objectives and Assessment Criteria," MALAKOFF, France, 2013.
[9] A. Washington, R. A. Clothier, and B. P. Williams, "A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems," *J. Air Transp. Manag.*, vol. 62, pp. 18–33, 2017.
[10] A. Washington, R. A. Clothier, B. P. Williams, and J. Silva, "Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems," in *17th Australian International Aerospace Congress: AIAC 17, Melbourne, Vic, Australia*, 2017, pp. 611–618.
[11] FAA, "Advisory Circular 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes.," 2011.
[12] FAA, "Advisory Circular 25.1309-1A, System Design and Analysis," US Department of Transportation, Federal Aviation Administration, 1988.
[13] R. A. Clothier and P. P. Wu, "A Review of System Safety Failure Probability Objectives for Unmanned Aircraft Systems," in *11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability (ESREL 2012) Conference, Helsinki*, 2012.
[14] SAE ARP 4754A, "Guidelines for Development of Civil Aircraft and Systems." SAE International, 2010.
[15] NATO Standardization Agency, "AEP-83, Light Unmanned Aircraft Systems Airworthiness Requirements," 2014.
[16] EASA, "E.Y013-01 Policy Statement Airworthiness Certification of Unmanned Aircraft Systems (UAS)," 2009. (Online). Available: https://easa.europa.eu/system/files/dfu/E.Y013-01_ UAS_ Policy.pdf. (Accessed: 23-Oct-2015).
[17] JAA/EUROCONTROL, "UAV Task-Force Final Report: A concept for European regulations for civil unmanned aerial vehicles (UAVs)," 2004.
[18] R. Clothier, B. P. Williams, J. Coyne, M. Wade, and A. Washington, "Challenges to the Development of an Airworthiness Regulatory Framework for Unmanned Aircraft Systems," in *16th Australian International Aerospace Congress (AIAC 16)*, 2015, pp. 87–98.
[19] R. A. Clothier, J. L. Palmer, R. A. Walker, and N. L. Fulton, "Definition of an airworthiness certification framework for civil unmanned aircraft systems," *Saf. Sci.*, vol. 49, no. 6, pp. 871–885, 2011.
[20] R. A. Clothier, N. L. Fulton, and R. A. Walker, "Pilotless aircraft: the horseless carriage of the twenty-first century?," *Journal of Risk Research*, vol. 11, no. 8. pp. 999–1023, 2008.
[21] M. Elbanhawi, A. Mohamed, R. Clothier, J. L. Palmer, M. Simic, and S. Watkins, "Enabling technologies for autonomous MAV operations," *Prog. Aerosp. Sci.*, vol. 91, pp. 27–52, 2017.
[22] R. Clothier, "Turning Hype into Reality: Unmanned Aircraft Systems and the Challenges Ahead." AAUS, 2016.
[23] Department of Defense, "Unmanned Aerial Vehicle Reliability Study," United States of America, 2003.
[24] SAE ARP 5150, "Safety Assessment of Transport Airplanes in Commercial Service," 2013.
[25] E. T. Jaynes, *Probability Theory: The Logic of Science*. Cambridge University Press, 2003.
[26] H. Dezfuli, D. Kelly, C. Smith, K. Vedros, and W. Galyean, "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis," *NASA/SP-2009-569*, 2009.
[27] T. Perez, "Ship seakeeping operability, motion control, and Autonomy - A Bayesian Perspective," *IFAC -PapersOnline*, pp. 217–222, 2015.
[28] T. Perez, R. A. Clothier, and B. Williams, "Risk-management of UAS Robust Autonomy for Integration into Civil Aviation Safety Frameworks," in *Australian System Safety Conference (ASSC 2013)*, 2013, pp. 37–45.
[29] S. Guarro, "Risk assessment of new space launch and supply vehicles," in *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, 2012, pp. 5157–5164.
[30] S. D. Guikema and M. E. Pate-Cornell, "Bayesian Analysis of Launch Vehicle Success Rates," *J. Spacecr. Rockets*, vol. 41, no. 1, pp. 93–102, 2004.
[31] United States Nuclear Regulatory Commission, "Reactor safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," 1975.
[32] E. Ancel, F. M. Capristan, J. V. Foster, and R. C. Condotta, "Real-time Risk Assessment Framework for Unmanned Aircraft System (UAS) Traffic Management (UTM)," in *17th AIAA Aviation Technology, Integration, and Operations Conference,Denver, Colarado*, 2017.
[33] L. C. Barr, R. L. Newman, E. Ancel, C. M. Belcastro, J. V. Foster, J. K. Evans, and D. H. Klyde, "Preliminary Risk Assessment for Small Unmanned Aircraft Systems," in *17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, Colarado*, 2017.
[34] B. J. M. Ale, L. J. Bellamy, R. van der Boom, J. Cooper, R. M. Cooke, L. H. J. Goossens, A. R. Hale, D. Kurowicka, O. Morales, A. L. C. Roelen, and J. Spouge, "Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart," *Reliab. Eng. Syst. Saf.*, vol. 94, no. 9, pp. 1433–1441, 2009.