Thank you for downloading this document from the RMIT Research Repository.

The RMIT Research Repository is an open access database showcasing the research outputs of RMIT University researchers.


Citation:

See this record in the RMIT Research Repository at:

Version: Accepted Manuscript

Copyright Statement: © 2008 Taylor & Francis

Link to Published Version:
http://dx.doi.org/10.1080/13669870802323353
Pilot-less Aircraft: the Horse-less Carriage of the 21st Century?

Reece A. Clothier a,*, Neale L. Fulton b, Rodney A. Walker a

a Australian Research Centre for Aerospace Automation (ARCAA), Queensland University of Technology (QUT), GPO Box 2434, Brisbane, Queensland 4001, Australia

b Commonwealth Scientific and Industrial Research Organisation (CSIRO), Mathematical and Information Sciences, Canberra, Australia

* Corresponding author. Tel.: +61 7 3138 1362; fax: +61 7 3138 1516
E-mail addresses: r.clothier@qut.edu.au (R. Clothier), neale.fulton@csiro.au (N. Fulton)
ra.walker@qut.edu.au (R. Walker)

Abstract

This paper identifies recurring issues in the regulation of new technologies through an historical review of the risk management of automobiles in the 1800’s. Parallels are drawn between the regulation of early automobiles and that of the regulation of Unmanned Aircraft Systems (UASs) today. It is found that many of the regulatory challenges facing UASs are analogous to those which faced the automobile industry more than a century and half ago and that the need for informed and objective decision making in policy development is reinforced. A systems engineering approach, based on general systems theory and decision-based design principles, is then proposed as a means for improving the objectivity, transparency and rationality in the risk management decision making process. An example risk management decision making is given within the context of a small UAS operating over a populated area. The results obtained from this case-study illustrate how even simple analysis can support the decision making process and highlights some of the potential challenges in the regulatory approach currently applied to UASs.

Keywords

UAS, UAV, Risk Management, Regulation, Decision Based Design, Systems Engineering
1. Introduction

Unmanned Aircraft Systems (UASs) or “pilot-less aircraft” are not a new technology. The first successful flight of a powered UAS occurred in 1918; just over a decade after the pioneering flights of the Wright Brothers (Newcome, 2004). However, unlike Human-Piloted Aviation (HPA), the limitations of available technologies (and perhaps a lack of foresight) hindered their ongoing development. The realisation of a potentially viable UAS industry has only come about through the availability of enabling technologies, in particular: digital processors and the Global Positioning System (GPS). The business case for UAS in a range of military and civil/commercial applications will continue to strengthen as the cost of development falls and their capability increases, a trend reflected in UAS market growth forecasts (Zaloga et al., 2007). However, there are a number of challenges that still need to be addressed before a viable UAS industry can become a reality.

History has shown us that some of the greatest obstacles facing the realisation of a new technology are not always technical in nature but are often related to its integration into Society. There are a number of political, economical and sociological issues governing the acceptance and integration of a new technology. One issue of particular importance is the management of any associated risks.

Society is becoming increasingly risk aware (Slovic, 1987) and as a direct consequence there is growing opposition towards the introduction of new technologies and their associated risks. The hazards of UAS operations present risks to a number of entities (i.e., people, environment etc) and it is the Authors’ belief that the greatest challenge facing the realisation of a safe, yet viable UAS industry is the development of effective strategies to manage these risks.

The progression of knowledge is an incremental process and it is through experiences (particularly failings), experimentation and historical observations that Society furthers its understanding in a particular field. Therefore, much insight into the issues concerning the risk management of new technologies can be gained through observing the risk management of previous technologies.

Many parallels can be drawn between the issues concerned with the risk management of “horse-less carriages” in the 1800s and those issues concerned with the risk management of “pilot-less aircraft” today. This leads to an interesting question: if it can be argued that there have been no significant changes in the fundamental behaviour of Society towards new technological risks; why has the science of risk management not addressed the recurring issues concerning new technologies? The following section, §2 A Lesson in History? The Regulation of the “Horse-less Carriage”, explores some of these recurring
issues through a historical comparison between automobiles and UASs. The third section, \textbf{§3 An Engineering Design Perspective}, discusses the application of engineering design practices, based on general systems theory (Boulding, 1956) and decision-based design principles (Marston and Mistree, 1997; Mistree \textit{et al.}, 1990), as one means for improving the objectivity, transparency and rationality in the risk decision making process. The approach assists in the characterisation of the decision scenario; providing boundaries of rationality to aid decision makers. A theoretical decision scenario of a UAS operating over an inhabited area is then used to illustrate how the application of engineering design principles can support rational decision making.

2. \textbf{A Lesson in History? - The Regulation of the “Horse-less Carriage”}

It is believed that the inception of the “horse-less carriage” was on the sketch-pad of Da Vinci but it was not until 1769 that Nicolas Joseph Cugnot developed the first self-propelled steam driven vehicle (Flink, 1988). One year later, Cugnot developed a tricycle vehicle capable of carrying four passengers. Ironically, it is believed that in that same year Cugnot also became the first person to be involved in an automobile accident, when his steam-driven vehicle crashed into a stone wall (Fallon and O’Neill, 2005). It was not until the mid-to-late 1800s that steam-driven horse-less carriages reached a level of technological maturity that saw their increasing use on public roads. The development of the battery in 1859 by Planté and its further refinement by Faure, marked the beginnings of the electric automobile. Electric automobiles were poised to overcome many of the frailties of their steam-driven counterparts but it was the advent of the gasoline internal combustion engine in the twilight of the 1800’s by Otto, Daimler, Benz and Maybach that marked the true dawn of the “horse-less” age. As the number and performance of horse-less carriages on public roadways increased, so too did the opposition towards them.

Risk management of automobiles was taking place well before the revolutionary advancement of the internal combustion engine. In the UK, an example of these measures was the Locomotive on Highways Act of 1865 often referred to as the "Red Flag Law" (Flink, 1988; Richardson and O’Gallagher, 1977). The Act stipulated that all self-propelled vehicles on public highways in country areas be limited to a maximum speed of four mph (two mph in towns) and that they be preceded by a man on foot carrying a red flag or lantern (Richardson and O’Gallagher, 1977).

The primary argument justifying the passing of the Act was the concern for the safety of other road users. However, it is interesting to note that the first widely-known automobile fatality did not occur until
1869 (Fallon and O'Neill, 2005), four years after the introduction of the Act. Ironically, the person fatally injured was a passenger of an automobile, the protection of whom was not the primary focus of the Act. It was not until August 1896, some 31 years after the introduction of the Act, that the first non-occupant fatality due to the operation of an automobile was recorded in the UK. Based on these facts, it could be argued that the passing of the Act was proactive in the safety-management of other road users. However, to further weaken the justification for the Act on the grounds of safety: the braking systems on early automobiles were superior to that of horse-drawn carriages and automobiles were not subject to the often unpredictable (Lee, 1998) and uncontrollable desires of a horse (Flink, 1988). So why did the Act pass? The true agenda behind the introduction of the Act were ‘hidden’ sociological, economical and political factors.

In the early-to-mid 1800’s, there was much resentment towards the presence of horse-less carriages on public roadways. The noisy and smelly machines often frightened horses which were used by the majority of other road users. The high cost of early-automobiles created an economic-divide in their ownership and consequently the general public viewed automobiles as merely a nuisance-toy for the rich. Automobiles also damaged the roadways, which had not been designed to accommodate such heavy and fast moving vehicles. In addition, it is likely the public’s limited knowledge and general inability to understand the complexities of automobile technologies contributed to an increased perception of the dangers. These factors and many more, created a general air of hostility towards automobiles. This hostility was used to the advantage of the true proponents behind the passing of the Act; those industries threatened by the prospect of a competing transportation technology (primarily the horse-drawn carriage, tram and rail industries (Flink, 1988; Setright, 2004)).

The passing of the “Red Flag Law” had significant ramifications for both the industry and the Society it was trying to protect. For more than 30 years the ‘discriminatory’ (Flink, 1988) Act ‘stultified’ (Flink, 1988) the further development of the automobile in the UK, leaving the United States of America, France and Germany to reap the many benefits from pioneering in automobile technologies.

The Act was finally amended in 1878, removing the need for a red flag and reducing the distance a man should travel ahead of the automobile to 20 yards. However, this small relaxation came at a cost. The amended Act stipulated that the driver was required to stop the automobile at the sight of a horse and that the automobile should make no emissions in case it should frighten horses using the road. It was not until the passing of the Locomotives on High Ways Act of 1896, more than 30 years after the passing of the
“Red Flag Law”, that there was a significant relaxation granted to horse-less road users. The 1896 Act, commonly referred to as the “Emancipation Act”, recognised the growing use of automobiles as a means of personal transportation (Clapton, 2004) by establishing two categories of automobile: light locomotives and carriages, and those automobiles which exceeded three tonnes. Under the Emancipation Act, the maximum speed for light vehicles was raised to 14 mph and light vehicles were no longer required to be proceeded by a man on foot. This relaxation marked a turning point for the UK automobile industry and was celebrated by the “Emancipation Day” motorcar race between London and Brighton (Flink, 1988).

The next major development in regulations was the 1903 British Motor Car Act which introduced vehicle registration and driver licensing as well as penalties for recklessness, negligence or speeding. It was not until the 1930 Road Traffic Act that comprehensive regulations on the classification, construction, equipage, weight, driver licensing, insurance and guidance for road users (the Highway Code) were defined. This later Act forms the basis for modern automobile regulations in the UK.

In 2005, traffic accidents on Great Britain roads caused 3,201 fatalities and 28,954 serious injuries (DFT, 2006). More than 800 of these fatalities were other road users, pedestrians or cyclists. It cannot be assumed that all 800 of these fatalities were the result of an interaction with an automobile but with these figures in mind; there is debate as to whether current regulations are truly effective despite nearly a century and a half of progressive refinement.

2.1 The “Horse-less Carriage” of the 21st Century?

Clear parallels can be drawn between the situation which faced “horse-less carriages” in the 1800’s and that which faces “pilot-less aircraft” today. A fully autonomous UAS essentially removes a component of an aircraft subject to error, the pilot, much in the same way the temperamental and unpredictable horse (Lee, 1998) was replaced by an engine.

Before making further comparisons it is important to discuss one major difference between the risk paradigms of the two technologies. This is in the visibility of the benefits to Society. For automobiles the relationship between benefit and the primary individuals at risk (the occupants) is fairly apparent. However, for UASs the visibility of the benefits to the primary individuals at risk (people on the ground) is much more difficult to show. This difference has an impact on the acceptability of the risks to Society. However, in the early years of the automobile the immediate benefits of the industry were not as apparent as they are today. The public’s tolerance of the risks changed markedly when automobiles became recognised as a viable form of personal transportation. Therefore, comparisons can still be made between
the regulatory process as applied to early automobiles and that of the regulatory process applied to UASs today. However, in today’s risk aware Society, addressing the broader issues concerning the acceptability of the risks of UAS operations may prove a much more significant challenge.

Analogous to the introduction of automobiles to public roadways, UASs are a new user within the National Airspace System (NAS); an established system designed to meet the needs of Human-Piloted Aircraft (HPA) (DeGarmo, 2004). The introduction of UASs to this system creates an entirely new risk management paradigm and this has potential ramifications on:

1. The safety-performance of the NAS (e.g. changes in the level of risks to other airspace users)
2. The efficiency of the NAS (e.g. increased complexity and congestion)
3. The NAS environment (e.g. increased contrails, emissions and noise)

UASs compete with existing NAS users for their relative contribution to the three factors listed above. The UAS industry is also a commercial competitor to existing NAS users in a number of applications. Similar to the regulation of early automobiles, these factors and a range of other political, social and economic factors, will influence (either directly or indirectly) the development of safety policy. Ideally, the development of such policy should be governed by the risks presented to Society, independent of such influences.

The primary risks to Society due to the operation of UASs are those associated with the hazards of midair collision and a discontinuance of flight over a populated region (JAA/EUROCONTROL 2004; Brunet et al., 2004). These hazards present a risk to people onboard other aircraft and to people and property on the ground, respectively (JAA/EUROCONTROL 2004; Brunet et al., 2004; Clothier and Walker, 2006; Grimsley, 2004). The following sections discuss the current and proposed regulation strategies for the management of these two hazards, and the potential ramifications these strategies have on industry and Society.

2.1.1 The Risks to Other Airspace Users

Integration into the NAS requires UASs to demonstrate, at minimum, an equivalent see-and-avoid capability to that currently provided by a pilot onboard a conventional aircraft. As described in (CASA, 1988; ICAO, 1990), the see-and-avoid function requires the pilot, under suitable visibility conditions, to maintain a visual lookout for other aircraft and if necessary, initiate manoeuvres to avoid a potential collision scenario. The responsibility for collision avoidance ultimately resides with the pilot, irrespective
of any third party separation services (e.g., those provided by air traffic control) or technology-based separation aids (e.g., Traffic Alert and Collision Avoidance System).

UASs currently lack a sense-and-avoid capability equivalent to the see-and-avoid function (CASA, 2002; JAA/EUROCONTROL 2004; OSD, 2005). Until such a capability is available, the risks due to the hazard of a midair collision have been managed by placing restrictions on where UAS operations can take place. These restrictions include confining UAS operations to: volumes of airspace segregated from all other airspace users, volumes of airspace with known or controlled traffic distributions, or to volumes of airspace known to have extremely low traffic interactions (such as oceanic areas). In striking similarity to the requirement for an automobile to be preceded by a man on foot with a red flag; safety authorities may also require a UAS to remain under the continual visual surveillance of a human observer located in a chase aircraft or situated on the ground (FAA, 2008). Mandating such a requirement renders most non-segregated UAS operations impractical and economically unviable.

The Australian Civil Aviation Safety Authority (CASA) does not mandate an equivalent see-and-avoid capability for civil/commercial UAS operations outside of segregated airspace. The CASA has adopted a receptive risk management policy open to a range of risk management approaches which can permit restricted access to the NAS. Whether a sense-and-avoid capability is required is at the discretion of the regulator who must assess, on a case-by-case basis, the acceptability of the level of residual risk presented to other airspace users. In the short-term the operational restrictions mandated by CASA are tolerated by the UAS operator. However, the routine and unrestricted access of UASs to the NAS is unlikely to come about until an equivalent sense-and-avoid capability has been developed.

2.1.2 The Risks to People and Property on the Ground

A discontinuance of flight presents a risk to people, property, and other entities of value on the ground. In 2006, the first widely-known civilian fatality due to the operation of UASs was recorded when a UAS crashed in the Democratic Republic of Congo, killing one civilian and injuring three others (La Frachi, 2006). Unfortunately, as the number of UASs operating over populated regions continues to increase, so too will the frequency of such mishaps.

UASs currently exhibit mishap rates of up to two orders of magnitude greater than that exhibited by HPA (OSD, 2005). A major factor contributing to these high mishap rates is the low reliability of the system (which encompasses the airborne platform, communications links, ground control and ‘human’ elements (OSD, 2005; DeGarmo, 2004)). The limited mishap data available for UAS also cite human
factors, poor maintenance and operational procedures as other significant contributing factors (OSD, 2004; Williams, 2004). In general, this high mishap rate can be attributed to a lack of airworthiness which is traditionally obtained through a body of prescriptive regulations (OSD, 2002). These regulations define the approved standards and procedures to which UASs should be designed, manufactured, maintained and operated. As it stands, no consensus has been reached on the definition of airworthiness regulations specific to UASs. In the absence of prescriptive airworthiness regulations, regulators have placed restrictions on the operation of UASs near populated regions and/or have mandated compliance to existing standards developed for HPA.

Conditions mandated under CASR Part 101 (CASA, 2002) permit some UAS operations in the NAS under certain operational restrictions. However, all UASs must be certificated against an approved body of standards in order to operate over a populated area (a requirement for many commercial applications). The Federal Aviation Administration (FAA) currently requires all civil/commercial UASs to obtain certification against a suitable body of standards before approval for operations within the NAS will be considered (FAA, 2008). At this point in time, neither the FAA nor CASA have defined prescriptive standards specific for the certification of UASs. At the time of writing the only mechanism for civil/commercial UAS operations in the NAS is via a special certificate of airworthiness in the experimental category. Conditions under this certificate preclude operation for commercial reward and include substantial operational restrictions. These can include restrictions on the regions over-flown, on the minimum altitude of operations and the carriage of mitigation systems not currently prescribed for HPA (e.g., parachute systems). Effectively these restrictions make the commercial operation of UASs over inhabited regions impossible.

No objective methodology justifying the application of restrictions is provided; subsequently the restrictions are mandated based on the perceived levels of risk for the operation. In addition there is much ambiguity in the regulations (e.g., CASR 101.025 - the definition of a “populous area” (CASA, 1998)) which leaves room for interpretation. These factors can lead to the inconsistent management of the risks.

One approach is to base prescriptive certification regulations for UASs on those mandated for HPA. However, the existing standards and regulatory framework for HPA may not address the unique economical, technical and operational aspects of the UAS risk paradigm. The primary concern behind the definition of the existing regulations is the protection of people onboard the aircraft, something no longer relevant to UASs. For HPA, system reliability requirements are largely considered independent of the
intended operation (Haddon and Whittaker, 2002) and are therefore considered a simple function of the
“number of seats” onboard the aircraft. For UAS, the degree of risk is a function of both the system and
the environment it operates in and thus the required level of dependability of a UAS cannot be considered
independent of its intended operation. The existing “one size fits all” (McGeer et al., 1999) regulation that
mandates a ‘blanket’ level of reliability, may not be the most effective approach for the regulation of
UASs. This is particularly the case for small UASs or those UAS operations where the risks can be
considered negligible (e.g., remote or oceanic areas etc). Existing regulations may not be applicable to
UASs (e.g., requirements on crash-worthiness) and may not address unique elements of UASs (e.g.,
ground stations, flight termination systems and autonomous software systems etc). In addition, it may not
be practicably possible, or economically feasible to certify some UASs to existing standards when
considering the physical limitations of aircraft and the commercial drivers behind their applications,
respectively.

2.1.3 The Regulation of UAS; A “Red Flag” Policy?

Some stakeholders believe that UASs present an unacceptable risk to other airspace users and people
and property on the ground. As a result, safety regulators have put in place temporary and somewhat ad-
hoc measures to mitigate the perceived risks that, much like the “Red Flag Law”, lack objective
justification. Where the regulations do not effectively preclude the operation of UAS altogether; they
impose substantial restrictions. These restrictions have a significant impact on the business case
supporting the application of UASs over competing technologies and prevent the operation of UASs in
many widely-beneficial applications.

However, one cannot critique the regulator too heavily. It is the regulator’s responsibility to ensure
the safety of Society and it can be argued that the current regulations are more than satisfying this
obligation. It could also be argued that the ‘precautionary’ (UN, 1992) measures in place are justifiable
considering the general lack of objective knowledge of the risks of UAS operations that is available to
regulators. With this in mind, it is important to remember that such precautionary measures should only
remain whilst there is a lack of objective evidence to prove otherwise.

The slightly more receptive regulatory stance adopted by CASA is the envy of the UAS industry
around the world. To some extent this more receptive approach is made possible because of the unique
aspects of Australia’s operating environment; specifically the relatively empty skies and the distributed
nature of its population. In the short term this receptive stance, like the stance adopted by France, USA
and Germany in the regulation of early automobiles, may allow Australia to capitalise on some segments of the developing UAS industry. However, this window of opportunity is closing. The current regulations are by no means a solution to the long-term needs of the industry. Ultimately, UASs require a degree of operational freedom within the NAS comparable to that of HPA. This will only come about through the development of effective regulatory policy that “regulates with respect to risk”.

2.2 Thinking Beyond the Horse

The risk management of UAS operations within the NAS has been based on the high level requirements for transparency, compliance and equivalency to that of HPA operations (JAA/EUROCONTROL 2004). This immediately raises an important question: are these over-arching requirements valid? Should UASs be required to conform to the existing risk management system or should a new system be developed with all users in mind? Arguments supporting the former include:

1. UASs represent a small proportion of airspace users
2. There is much maturity in the current system which delivers an acceptable level of safety

To address the first of these arguments, like automobiles in the 1800’s, UASs currently constitute only a small fraction of airspace users and thus have very little sway when compared to that of the revenue generating passenger and freight transportation industries. However, it is likely that this scenario will change as regulations evolve and the business cases supporting the UASs market strengthen. After all, it only took automobiles just over a century to revolutionise Society’s concept of transportation, a concept which had been instilled for thousands of years.

Secondly, the current airspace system was designed around the performance of a human pilot (e.g., see-and-avoid, visual/instrument flight rules etc). Forcing UASs to conform to this system may do more harm than good. A notable proportion of the accidents attributed to automobiles were due to the fact they were forced to use narrow roadways designed for a smaller number of slower road users (Granville-Edge, 1926). It was not until 1906, approximately 40 years after the "Red Flag Law", that regulators acknowledged that in order to ensure the continued safety and convenience of pedestrians (due to the proliferation of automobiles), it would require the regulation of pedestrian traffic (Ishaque and Noland, 2006). Inevitably, the existing road system and its users were required to accommodate automobiles for the safety and efficiency of all.

Guiding principles such as compliance and equivalency to existing practices, standards and regulatory frameworks may preclude the exploration of safer and more efficient long-term risk...
management systems. Thus the entire regulatory and airspace systems should be re-evaluated with a ‘shared’ operating concept in mind. UASs are a fundamentally new aviation technology, the effective regulation of which may require a fundamentally new approach. However, despite the perceived urgency in the need for regulations, stakeholders should proceed with caution. The promulgation of ineffectual or inappropriate regulations could present an even greater challenge to the UAS industry than the precautionary regulations currently in place.

The historical comparison highlights recurring issues in the risk management of new technologies. In particular: the concept of safety and its management will always embody divergent perspectives and elements of subjectivity, potentially leading to the inappropriate or the ineffective management of the risks. Therefore the decision making process should focus on the communication of rational and objective arguments. It is important to note that such a focus does not guarantee stakeholder consensus or the broader acceptance of a new technology. However, such a focus does support decision making more resilient to such influencing factors. The following section discusses one possible approach supporting such resilience, through the application of philosophies used in systems engineering and design.

3. An Engineering Design Perspective

In 2003, controversial and broad changes were proposed in the management of regional airports in Australia, summarised in (CASA, 2004). Utilising principles drawn from engineering design, stakeholders for Broome International Airport provided a rational argument justifying a range of alternative risk management proposals (Emery et al., 2005). The arguments put forward overcame the many political and external influences; resulting in changes to the proposed regulations (CASA, 2005). This example highlights the potential benefits of the application of engineering design principles to the Risk Management Decision Making Process (RMDMP). The following section (§3.1) explores the application of these principles within the context of the UAS RMDMP. These principles are then applied to a case-study decision scenario (§3.2).

3.1 The Decision Making Process and the General Systems Hierarchy

The definition of a regulatory framework is the outcome of a RMDMP; a process analogous to the decision making process in engineering design. Mistree et al.(1990) observes that decisions in engineering design are:

1. Invariably multi-levelled and multi-dimensional in nature,
2. Involve multiple sources of information from varying disciplines, and are
4. That the decision space is often open, and
5. That there is often no singular, unique or optimum solution to any single decision problem

Mistree et al., (1990) also observes that the information required for decision making:
1. May be scientific (hard, objective) or subjective (soft, judgemental), and
2. May not always be available

Based on the observations above, there are many similarities between the challenges faced in decision making in engineering design and those currently facing the RMDMP for UASs and this section formally describes the application of this approach.

3.1.1 The UAS Risk Management Decision Making Process – A Black Box System?

Systems theory is most often applied in the management and design of complex technological systems or processes. A system is defined as:

“*A set of interrelated components which interact with one another in an organized fashion towards a common purpose.*” (Shishko and Chamberlain, 1995)

The RMDMP can also be described as a system. The components of a system can comprise people, organisations, facilities, equipment, product or resources, and in the case of the RMDMP for UASs, these components interact with the objective of establishing regulations acceptable to all stakeholders. As mentioned in the previous section, the interactions and components which comprise the RMDMP are uncertain. Therefore, the entire process could be considered a black box system; a system where the inner workings are hidden from the outside observer, Fig. 1. The UAS RMDMP could be considered even less observable than a black box system. This is because all of the inputs to the decision process are not entirely known. As a consequence, it may not be possible to completely characterise the system based on the observation of its outputs alone.

![Fig. 1. Black box representation of the Risk Management Decision Making Process (RMDMP)](image-url)
There needs to be transparency in the RMDMP in order for stakeholders to have confidence in the objectivity and integrity of safety policies mandated. Ideally this process would be described as a “white box” system; where the interactions between internal components are completely visible to the outside observer and thus the relationship between the inputs (the risks, benefits and costs) and the outputs (safety policy) are comprehensibly known. However, the RMDMP will always involve stakeholder discourse and will always be subject to the influences of stakeholder perceptions and desires, and the political, social and economical climate the entire process occurs in. Thus attainment of a “white box” process may be an unrealisable objective. A more realistic objective is not to strive for complete transparency in the RMDMP but to move from opacity to a degree of translucency.

3.1.2 Moving from Opacity to Translucency

Boulding’s (Boulding, 1956) General Hierarchy of Systems (GHoS) is a multi-disciplinary theory describing the theoretical arrangement of abstracted systems based on the complexity of fundamental phenomena. Any RMDMP essentially comprises a hierarchy of knowledge and decisions, and therefore can be described in terms of the different levels of the GHoS.

The GHoS describes a “system of systems”. Within the context of a RMDMP this is where decisions made at higher levels of the hierarchy will ultimately translate to systems residing at lower levels within the hierarchy. For example, decisions with regard to the safety of UASs (a concept at the level of social sciences) will translate to standards and procedures relating to the dependability of UASs, their operation and custodianship (the levels of physical sciences: frameworks, clockworks and thermostats). Systems at the level of physical sciences are the ultimate ‘subjects’ of the outputs from the RMDMP. A RMDMP described in this manner follows a top-down or deductive process.

Our understanding and ability to characterise processes residing within the social levels of the GHoS is limited. As a consequence it is difficult to show traceability between the decisions made at these upper levels (e.g., the requirement for an equivalent level of safety (CASA, 2002; JAA/EUROCONTROL 2004; CAA, 2004; OSD, 2005) to the requirements at lower levels (e.g., standards on the design of UASs).

One of the advantages in viewing the RMDMP from the perspective of Boulding’s GHoS is that it also supports a “bottom up” approach. A “bottom up” approach utilises the wealth of theoretical knowledge and data at the lower levels of the GHoS (the levels of physical sciences) to provide a better understanding of the behaviour of systems that reside in the upper tiers of the GHoS (the uncertain levels of social sciences). Specifically, the objective measure of the risks and their relationship to physical
technological systems and operational environments can be used to establish rational constraints and bounds on the Risk Management Decision Space (RMDS).

### 3.1.3 Establishing a Rational Decision Space (RDS)

It is common in engineering design scenarios for physical limitations in the systems to manifest themselves as constraints and bounds on a design space (Mistree et al., 1990). These constraints and bounds can be used to establish a “feasible design space” (Mistree et al., 1990). This feasible design space is separate from the “aspiration design space” which is defined by the goals of the design process (Mistree et al., 1990). Decision-Based Design (DBD) principles characterise the feasible design space by:

1. **Bounds** – the physical limits on input criteria: e.g., the finite amount of resources available for risk mitigation, or the maximum observable consequence for a particular hazard etc.
2. **Constraints** – relationships between input criteria: e.g., the relationship between cost of mitigation strategies and the level of residual risk, or the relationship between the takeoff weight and operating range for an aircraft etc.

... (Mistree et al., 1990)

A “Rational Decision Space” (RDS) analogous to the “feasible design space” in engineering design problems can be defined within the Risk Management Decision Space (RMDS) by identifying the bounds and constraints of objective decision-input criteria. An example two dimensional RMDS is illustrated in Fig. 2. The RDS in Fig. 2. is defined by the region enclosed by the bounds \((x_{\text{min}}, x_{\text{max}}, y_{\text{min}}, y_{\text{max}})\) and constraints \((C_1, C_2)\).

![Fig. 2 Rational Decision Space in a 2-dimensional Risk Management Decision Space](image-url)
3.1.3.1 The Risk Management Decision Space (RMDS)

The Risk Management Decision Space (RMDS) is the \( n \)-dimensional space defined by the \( n \) inputs to the RMDMP. As stated previously, not all of the inputs to the RMDMP are known or can be objectively characterised. However, studies in the field of risk management and social sciences have indicated that decisions made in relation to the acceptability of risks are a function of the perceived level of risk to entities of value to society, the potential benefits received in return for the hazardous activity, and the costs incurred in managing the risks (e.g., Starr et al., 1976). Therefore objective inputs to the RMDP for UASs would need to be defined in each of these three areas. The scope of this identification process should include numerous stakeholder perspectives (e.g., the risks the loss of a UAS has from the perspective of the UAS operator).

3.1.3.2 Bounds and Constraints

Bounds represent the limits on input criteria and can be established through formal risk analysis. The risk analysis process can draw on formal risk techniques, empirical data, modelling and expert judgement to identify and characterise boundaries and constraints between input criteria. In the context of establishing boundaries for the RDS, the objective of a risk assessment is to determine the potential range inputs to the RMDMP can take. Establishing the extremes of the risk scenario is a much easier problem to solve, as often the solution can be found within fundamental knowledge of physical sciences (GHoS – the realms of frameworks, clockworks and thermostats).

A constraint represents a relationship between input criteria which is required to be satisfied. At the levels of physical sciences, these constraints take the form of simple theoretical and analytical relationships, for example: fundamental theories in aerodynamics or physics.

A similar approach could be used to establish boundaries and constraints for the benefits of UAS operations (e.g. the use of economic studies (Zaloga et al., 2007)).

3.1.3.3 The Rational Decision Space (RDS)

The RDS is formed by the Cartesian product over the domain of input criteria. The design space is formed by setting the bounds and constraints of each individual decision input criterion (Fulton, 2002). The bounds and constraints serve as ‘fences of logic and rationality’ within which the subjective (and uncertain) decision function, \( f \), can move freely. Any decision scenario that resides outside these fences is driven by subjective or hidden inputs and must lie in the aspiration space of the stakeholders. Careful consideration should be given to the plausibility of such scenarios.
An example RMDS is shown in Fig. 3A. In some instances it may not be possible to establish all of the boundaries on the RDS. In such scenarios one or more dimensions of the RMDS may be open or unconstrained, as illustrated in Fig. 3B. Decisions across this dimension are often restricted by the needs or desires of the stakeholders (the aspiration space, refer §3.1.3.3). Not all boundaries or constraints can be evaluated with absolutely certainty. The level of certainty in a boundary or constraint depends on the mechanism/process and underlying data used in their evaluation. For example: boundaries or constraints established with a sound basis in theoretical lore (e.g., the formula for kinetic energy) or using absolute measures (e.g., maxima of a finite resource) will have a high degree of associated certainty. In order for decision makers to have confidence in the RDS, margins of uncertainty should be provided, as illustrated in Fig. 3C.

3.1.3.4 The Aspiration Space

The Aspiration Space (AS) is a region in the RMDS that reflects the desired states of the system, as illustrated in Fig. 3D. Unlike the RDS, it may not be possible to derive the boundaries of the AS in an entirely traceable and objective manner. Instead the bounds can be driven by perceptions, preferences and/or other processes residing in the social tiers of Boulding’s GHoS. Thus, an AS may not necessarily intersect the RDS, as illustrated in Fig. 3D.

Rational aspirations or Feasible Goals (FG) are those stakeholder aspirations which are transferable to realistic requirements on physical systems and operations, and reside in the region of intersection between an AS and RDS, Fig.3E.

Each stakeholder has unique preferences, goals and perceptions and subsequently, will have a unique region of aspirations within the RMDS. In cases where there is no common ground between stakeholder aspirations (as illustrated in Fig.3F), the decision function, $f$, should undertake a process of compromises within the bounds of the RDS. A Region of Consensus (ROC) is formed where there is some agreement between stakeholders (the regions of intersection between two or more ASs, as illustrated in Fig. 3G). The ideal decision scenario would be to have stakeholder consensus (a ROC) which intersects the RDS thus defining a region of Feasible Goals (FGs), Fig. 3H.
Fig. 3. Example RMDS scenarios. (A) RDS formed by constraints and bounds. (B) RDS without upper bound. (C) RDS with uncertainty in bounds. (D) RMDS with one Aspiration Space (AS$_1$) outside the bounds of the RDS. (E) RMDS with region of Feasible Goals (FG). (F) RMDS with two aspiration spaces (AS$_1$, AS$_2$) in contention. (G) RMDS with two aspiration spaces (AS$_1$, AS$_2$) and a Region of Consensus (ROC). (H) RMDS illustrating regions of FG (solid black line) and ROC (dashed black line).
3.2 Case-Study Scenario

The purpose of this case-study is to illustrate how the application of the perspective described in the previous section can assist the RMDMP. Many details and assumptions have been omitted in order to provide a concise example and thus any quantitative figures are purely illustrative.

Consider a theoretical decision scenario where a level of system reliability for a small UAS needs to be determined for a mission over an inhabited area. The UAS under consideration is loosely based on the Raven™ RQ-11B (Aerovironment, 2006). It is assumed that the UAS is operating over an area which has a uniformly distributed population density of 26.7 inhabitants per square kilometre. This is the average density for an “inner regional” area in Queensland, Australia (ABS, 2004).

3.2.1 Defining the Decision Space

The required level of system reliability is driven by the level of risk the UAS presents to the territories over-flown (people, property, environment etc). For this scenario, only one domain of consequence is considered, the consequence to human life and this is expressed in terms of the expected number of human casualties per flight hour of operation. The casualty expectation criterion (proposed by (JAA/EUROCONTROL, 2004) and (Grimsley, 2004)) is used purely for illustrative purposes, and is not recommended as a sole-metric for describing the risk of UAS operations. The other decision input variable is the System Loss Rate (SLR) per flight hour. A two-dimensional RMDS can be defined with the x-axis corresponding to the SLR and the y-axis corresponding to the casualty expectation.

3.2.2 Boundaries

Independent of any other factors, there is no theoretical limit on the minimum reliability of the UAS and therefore the RDS has no upper bound with respect to the SLR. However, it is unlikely a UAS manufacturer would design a system with a level of reliability less than that of the baseline system. The baseline SLR (assumed as 0.04 per hour) is used as the upper boundary (indicated in Fig. 4, with a vertical dotted green line).

Improvements in system reliability (reductions in the SLR) can be achieved through robustness in design, assurance, maintenance and operational practices. Ultimately the minimal practicably obtainable SLR, independent of any cost factors, is restricted by the physical and performance limitations of the UAS platform (i.e., available volume, mass, power etc) and the current availability of key technologies. For many UAS, it is not practicably possible to mitigate all single points of failure within the system, and
still have it capable of carrying a usable payload. Limitations in key technologies can also be used to
define boundaries on the RMDS. One example is the propulsion system which is a key single-point of
failure in many UASs (OSD, 2003). Increasing advancements in key technologies will tend to shift
technology-driven boundaries to the left (reducing the SLR), increasing the size of the RDS.

It is assumed that the size and performance of the small UAS under consideration and the availability
of alternative technologies would limit potential improvements in the SLR to a factor of ten below that of
the SLR of the baseline system. This is shown as a purple vertical line (dash-dot) in Fig. 4.

Rational bounds on the casualty expectation (represented on the y-axis of Fig. 4.) can be determined
by looking at the ability of the UAS to inflict damage to people on the ground.

The casualty expectation is a complex function of the SLR, failure modes of the UAS, distribution of
people exposed (in space and time) and the conditional probability that a person struck by the UAS is
injured. To establish the minimum and maximum of this complex relationship, two extreme cases were
examined using the simple casualty expectation formula presented in (Montgomery and Ward, 1995).

The minimum boundary on the casualty expectation is summarised in Eq. 1. Using inert-debris injury
curves (RCC, 2002; Lin et al., 2003), it can be observed that the kinetic energy of the candidate UAS in
its minimal operational configuration (e.g., stall speed and lowest take-off weight) is highly unlikely to
cause a fatal injury to a person (a probability of a fatal injury on the order of 0.02). A minimum lethal
area of 1.4 m² was calculated for a vertical failure mode. Substituting the minimum practicably obtainable
SLR of 0.004 per flight hour into Eq. 1, the minimum boundary on the casualty expectation can be
calculated as 3x10⁻⁹ fatalities per flight hour (illustrated in Fig.4 as a horizontal (dash-double-dot) black
line).

\[
CE_{\text{min}} (SLR) = SLR \times \rho \times LA_{\text{min}} \times Pr(\text{fatality | strike})_{\text{min}}
\]

\[
CE_{\text{min}} (SLR) = 7.6 \times 10^{-07} \times SLR
\]

The equation for the maximum boundary on the casualty expectation is summarised below in Eq.2.
The maximum boundary on the casualty expectation was calculated assuming maximum kinetic energy
under a maximum operational configuration (max speed and weight). The probability of a fatality given a
strike was calculated as 0.93 and the maximum lethal area (under a gliding failure mode) was calculated
as 31m². Using the baseline SLR, the maximum boundary on the casualty expectation was calculated as
3.08x10⁻⁵ (illustrated in Fig.4 as a dashed horizontal green line).
Equation 2

\[ CE_{\text{max}} (SLR) = SLR \times \rho \times L_{\text{max}} \times \Pr(\text{fatality} \mid \text{strike})_{\text{max}} \]

\[ CE_{\text{max}} (SLR) = 7.70 \times 10^{-03} SLR \]

3.2.3 Constraints

The minima and maxima constraints on the casualty expectation can be determined by evaluating Eq.1 and Eq.2, across the entire domain of the SLR (illustrated in Fig.4 by the solid diagonal red line and by the solid diagonal blue line, respectively).

3.2.4 Defining the Rational Decision Space

A RDS is formed by the region bounded by the minima and maxima constraints and the boundaries of the two input criteria, illustrated in Fig. 4.

Fig. 4 Formulation of the RDS
3.2.5 Defining the Aspiration Space

For this case study it is assumed that there are only three stakeholder groups involved in the RMDMP:

1. the UAS manufacturer/operator,
2. the aviation safety regulatory authority, and
3. the general public.

3.2.5.1 The UAS Manufacturer/Operator

It is assumed that the aspirations of the UAS Manufacturer/Operator are purely commercial in nature and thus the maximum commercially viable SLR (independent of any mandatory regulatory requirements) is driven by the costs of system attrition, insurance and deployment (transportation, maintenance, personnel etc). These costs must be kept to a minimum relative to the financial return from the successful completion of the mission. This simple economic relationship is described in Eq.3.

**Equation 3**

\[ \text{Max}\{\text{return}\} = \max\{RPHr - CPHr\} \]
\[ CPHr = SLR \times SC + DC + CE \times IC \]

where:

- \( RPHr \) – Customer service rate per hour of operation (assumed fixed at $2 000 an hour)
- \( CPHr \) – Costs per hour of operation
- \( SLR \) – System Loss Rate (assumed baseline rate of 0.04)
- \( SC \) – Initial system cost (assumed as $35 000 per air vehicle which increases by $10 000 for every order of magnitude improvement by reduction in the SLR from the baseline rate)
- \( DC \) – Deployment cost per hour of operation (assumed as $300 per hour)
- \( CE \) – Casualty expectation per hour of operation
- \( IC \) – Third party insurance (assumed actuarial cost per fatal injury of $1M)

This simple model assumes that improvements can be made in the reliability of the system through economic investment (not limited by the availability of technologies) and that the customer will pay a fixed price per hour of operation irrespective of the SLR.
A plot of the economic model described by Eq.3 is provided in Fig. 5. The magnitude of the independent variables of the IC (dotted black line), SC (dash-dot purple line), and the RPHr (dashed red line) are shown in Fig. 5. The total CPHr as per Eq.3 is represented in Fig. 5 by a solid blue line.

It can be observed in Fig. 5 that the cost of system attrition (the SC) dominates the CPHr and not the actuarial costs of insuring against a third party casualty. This is due to the extremely low risk of a casualty resulting from an in-flight loss of the system. As the SLR decreases the CPHr approaches that of the DC ($300 per hour). The point of minimum commercial viability is the point where the CPHr equals that of the PRHr. This point occurs when the SLR is less than or equal to $5\times10^{-02}$ per flight hour. It is assumed that the region of commercial viability defines the AS of the UAS manufacturer/operator.

![Fig. 5. Economic model driving UAS manufacturer/operator aspirations](image)

### 3.2.5.2 The Aviation Safety Regulatory Authority

In keeping with the current regulatory authority standpoint on proposed UAS reliability requirements, the regulator is likely to adopt a ‘blanket’ reliability requirement. Paragraph 9.b.(3) of AC-23.1309 (FAA, 1999) describes the process used for deriving the system reliability requirements for different system failure condition categories. The allowable average probability per flight hour of a hazardous system
failure condition (a failure of the system potentially resulting in a serious injury or fatality) is between $1 \times 10^{-06}$ and $1 \times 10^{-05}$ per flight hour (FAA, 1999). Arbitrarily assuming that there are ten potentially hazardous system failure conditions for the small UAS (a similar assumption is made for catastrophic failure conditions in (FAA, 1999)), then the requirements for the overall SLR of the UAS must be between $1 \times 10^{-05}$ and $1 \times 10^{-04}$ per flight hour. These requirements define the boundaries of the AS for the aviation safety regulatory authority and are shown in Fig. 6.

![Fig. 6. Aspiration Space of the aviation safety regulatory authority](image)

### 3.2.5.3 The General Public

Characterising Society’s perception of the risks is a complex task and is the subject of much research, e.g., refer to (Slovic, 1987) and (Starr et al., 1976). For the purposes of this scenario, it is assumed that Society will not tolerate a level of risk more than that which is currently observed for HPA (i.e., an equivalent level of risk). A casualty expectation of $3.13 \times 10^{-08}$ involuntarily-exposed ground fatalities per flight hour was determined for HPA air carrier operations in the US (Clothier and Walker, 2006). No
minimum boundary is defined in order to reflect Society’s ultimate desire for “zero risk”. The AS for the
general public is illustrated in Fig. 7.

![Aspiration Space of the General Public](image.png)

**Fig. 7. Aspiration space of the general public**

The combined ASs of all three stakeholder groups is illustrated in Fig. 8. A ROC is formed where all
three ASs intersect (illustrated in Fig. 8 as the hatched region bordered by a black dashed line). This is the
region of the RMDS where the goals of all stakeholders are in agreement and a solution to the RMDMP
can be reached with minimum conflict in stakeholder objectives.
Fig. 8. The combined ASs of all three stakeholder groups

3.2.6 Summarising the Decision Space

The RMDMP can be characterised by the combination of the RDS and the ASs, illustrated in Fig. 9. A region of Feasible Goals (FGs) is illustrated as the area enclosed by a black dotted line. The ROC lies completely outside the bounds of the RDS, thus there are no FGs within the RMDS that meets the desires of all three stakeholder groups. Thus, like many decisions problems involving multiple stakeholders, a process of compromise is needed. However, a region of FGs is formed where the ASs of both the general public and the UAS manufacturer/operator intersect with the RDS, depicted as the black solid-shaded region in Fig. 9. In this region, the risk management is practically realisable, meets the economic desires of the UAS industry and satisfies the public’s desire for protection based on a comparative benchmark to the risks of HPA.

It can be observed that the AS of the regulator does not intersect the RDS at any point in the RMDS. The SLR requirements mandated under existing regulations for HPA are not realisable (i.e., lie outside the bounds of the RDS) in their application to the case study UAS operation. This is because of the practical and physical limitations of the UAS (e.g.: maximum take-off weight, available power etc –
factors in the realms of physical sciences). The SLR requirements are mandated independent of the operating environment (i.e., they have no direct relationship to the operating environment and thus the casualty expectation for the particular operation). This case study illustrates the disadvantages of using the existing certification approach of mandating blanket system reliability requirements. Effective regulation must acknowledge the shift of primary risks to entities external to the system.

![Case study decision space](image)

**Fig. 9.** Case study decision space

### 3.3 Summary

This section has discussed the application of systems engineering and DBD philosophies to the characterisation of a RMDMP.

The proposed approach supports informed decision making through objective reasoning whilst acknowledging the inherently subjective nature of the concept of risk and the RMDP. Boulding’s GHoS provides the theory to support a bottom up approach to the characterisation of the RMDS despite the absence of a complete understanding of the RMDMP. A bottom up approach capitalises on the wealth of knowledge of fundamental theories in the underlying physical systems to partition the RMDS into objective (the RDS) and subjective (the AS) regions. This ensures objective inputs to the RMDMP are independent of the subjective goals representing the preferences and beliefs of stakeholder groups. The
decision function, \( f \), remains a subjective process of stakeholder discourse, however the risk decision plane is no longer without bounds. Decision makers now have objective boundaries describing a set of rational and justifiable policy decisions. Not only does this provide greater transparency in the RMDMP but this approach provides information on the dynamics of the decision scenario, facilitating more effective communication and resource allocation strategies.

The case study demonstrated how even simple analysis can benefit the RMDMP and highlighted the potential challenges in adopting a “one sized fits all” regulatory approach for UASs.

4. Concluding Remarks

A lot can be learnt from the experiences of the past. Many parallels can be drawn between the risk management of “horse-less carriages” in the 1800’s and that of “pilot-less aircraft” today. Based on this comparison it is evident that many of the issues concerning the effective risk management of new technologies are still prevalent, despite the passing of more than 150 years.

With respect to the development of suitable regulatory policy for UASs, stakeholders should explore all possible solutions in a systematic and objective manner. It is acknowledged that in the interim it is “better to be safe than sorry” but such precautionary management strategies should only prevail in the absence of an analytical appreciation of the risks. It is also acknowledged that a complete analytical appreciation of the risks currently does not exist and thus there is need for research into the development of tools to support risk-informed decision making.

With more revolutionary aviation technologies on the horizon (e.g., personal air vehicles, routine sub-orbital and hypersonic aircraft), aviation regulators will need to overcome many of the recurring challenges in the development of regulations for new technologies. One proposed approach that could be used to help address these recurring issues may lie in the application of systems engineering and design philosophies. Whilst attaining an entirely objective and “white box” RMDMP may not be a realistic possibility, decision makers should instead look to utilise tools which add to the transparency of the RMDMP. It is hoped that such tools will help to ensure that “Red Flag” policies remain only as lessons in history.
Acknowledgements

The Authors would like to thank Dr Shane Dunn of the Defence Science and Technology Organisation (DSTO) for providing some of the inspiration behind this paper. The Authors would also like to acknowledge the contributions made by colleagues at the Australian Research Centre for Aerospace Automation (ARCAA), in particular Dr Duncan Campbell, and the Commonwealth Scientific and Industrial Research Organisation (CSIRO). Financial support for this research was provided by the Queensland State Government Smart State PhD Scholarship Program and Queensland University of Technology.

References

Emery et al. (2005) Design Aeronautical Study For Broome International Airport Terminal Airspace, Broome International Airport, Australia.


