ENCLOSURE 2

(WG I Report)

Note: The following details some of the work that led to the main elements in the main body of the final report. Therefore the wording for such elements as principles, terminology and definitions may differ from the main text where a consual view was established during the review process.

GENERAL, SAFETY AND SECURITY

2.1 SYSTEMS APPROACH TO REGULATORY DETERMINATION

2.1.1 Current regulatory differences

There is a difference today between the regulatory approach for the certification of aircraft and that adopted for the regulation of Air Traffic Control. In addressing the issue of the regulatory framework for UAV systems, aspects of both environments must be addressed.

The current aircraft certification process seeks compliance with a set of well defined standards known as the Joint Airworthiness Requirements (JARS). The air traffic environment is regulated by treating airports and air traffic centres as individual units and tasking the operators to provide Safety Cases to demonstrate their operations are safe.

A systems regulatory approach is not currently adopted at a high level and components within the system i.e. aircraft, airports, air traffic centres, personnel etc are administered and regulated independently.

The basic approach in this document is to bring into focus the various elements that exists for the total regulatory framework. In doing this care has been taken to ensure that all existing processes, standardas and documents are acommodated and that there is a common way that each issue can be addressed. This approach is illustrated in figure 2.1 showing the relationship between the major areas.

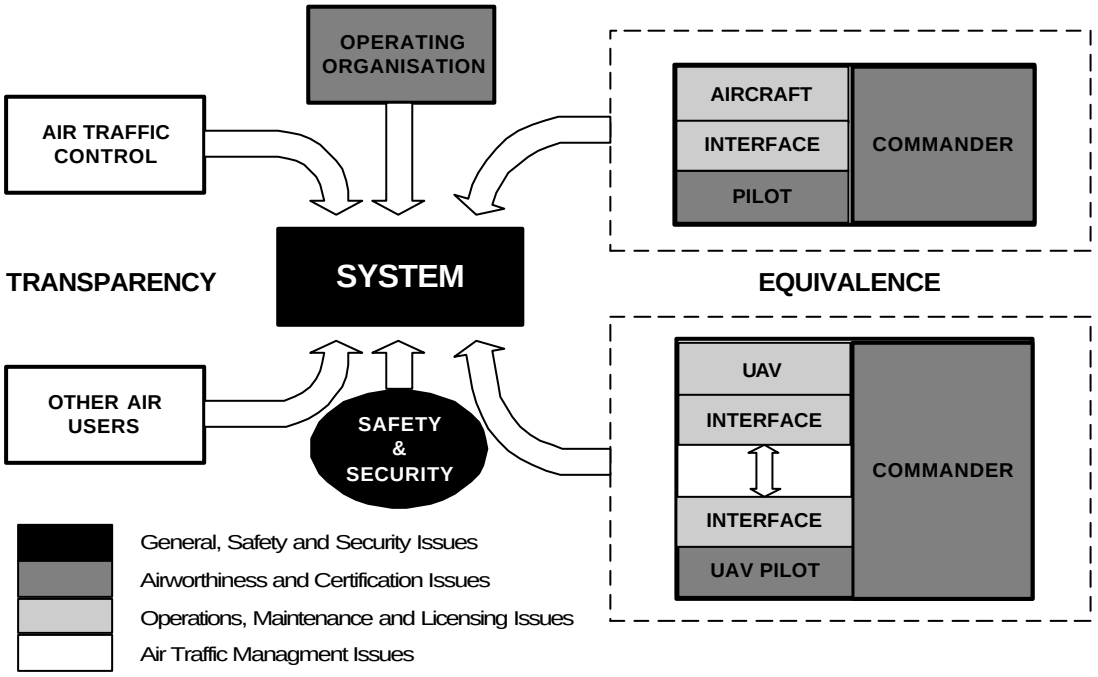


Figure 2-1 – Systems Approach to regulatory determination

At the top level a set of Principles has been adopted that guides the approach to the determination of a future regulatory framework. The two key principle areas are that of Equivalence and Transparency. The Principles that address equivalence are of great use when comparing manned and unmanned systems, both in the determination of airworthiness and in the operation of the air vehicle in the airspace environment. On the right of the diagram it can be seen that the manned and unmanned system is the same in all ways except the data link between the Pilot and the Air Vehicle control mechanism is extended beyond the phycial air vehicle.

The Principle of Transparency, on the left of the diagram, describes the interaction with ATM, Other Airusers etc. in that they should not be required to operate differently because of the UAV. This becomes useful when exploring operational issues.

A common set of terminolgy has been adopted throughout this document.

From a legal perspective there must always be a Commander who must bear ultimate responsibility for all flights within his control. They may or may not be the actual pilot of the aerial vehicle, whether it is manned or unmanned, where actual direct control may reside further down the management chain.

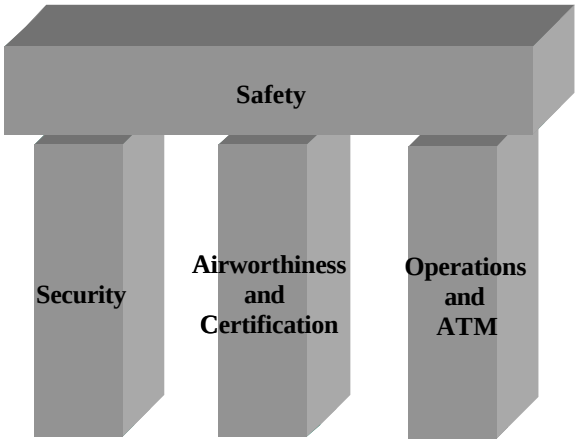
2.1.2 Key System Issues

The key system issue is Safety. Due to the nature of a UAV system, the safety aspects cover a greater area than that normally considered for manned systems. This wider scope brings into contrast the different approaches between the way aircraft and their operating environment are regulated.

A simple way to approach this is to regulate by Risk Analysis. Here it is the attainment of goals, where goals are associated with specific risks, that is important and not so much the process by which this occurs.

The prime focus for regulation is safety and the next section adopts and explains this high level concept. Security is dealt with as a sub-set of safety in order to ensure complete capture of all safety related issues although there are elements of security that may not be safety related. However Security is used, like Airworthiness and Certification to mitigate identified risks.

There are two main pillars to safe air operations; the safety of the underlying system and the safety of the air vehicle and its control mechanisms. Both these systems have been constructed upon Safety with Security, Airworthiness, Certification and Operations providing a "Tool Kit" with mitigation strategies. Over the past 100 years the regulations have



developed to provide guaranteed solutions to many of the extant risks and these should not be forgotten with UAVs. UAVs do not have 100 years of information to fall back on and therefore the mandated regulations should remain in place. With respect to the UAV System

the sections on Airworthiness and Certification and Operations should be viewed in two ways. Firstly as the interpretation of the Regulations applicable to the 100 years of knowledge and secondly as providing mitigation strategies with respect to a Safety Case specific to the system being certified.

2.2 UAV SYSTEM PRINCIPLES AND TERMINOLOGY FOR REGULATORY DETERMINATION

2.2.1 PRINCIPLES

(a) This section contains a set of principles applied within the report to enable a consistent approach to be established. The principles related to Equivalence and Transparency and are derived from the UK CAA document CAP 722 (ref n.) and more explanatory material on the reasoning behind all the Principles is to be found in Annex n.

2.2.1.1 General Approach

(a) Assumptions: All assumptions should be made explicit and challenged.

(b) Best practice: The development of UAV system regulations is an opportunity to improve the safety for all airspace users through the adoption of best practice from both non-UAV and UAV system developments and operations.

2.2.1.2 Equivalence

(a) Equivalent risk: UAV operations shall not increase the risk to other airspace users or third parties.

(b) Equivalent Compliance: UAV operators must ensure that their aircraft show an equivalent level of compliance with the rules that apply to manned aircraft.

(c) Equivalent Operations: UAV operators should seek to operate within existing arrangements.

2.2.1.3 Transparency

(a) The provision of an Air Traffic Service (ATS) to a UAV must be transparent to the Air Traffic Control (ATC) controller and other airspace users.

2.2.1.4 Regulatory compliance determination

(a) The determination of the airworthiness of a UAV is a separate function from the determination of UAV systems safe and secure operation.

2.2.1.5 Legal responsibility

(a) The legal responsibility for aircraft safe operation within a UAV System resides with a designated person.

2.2.2 TERMINOLOGY AND DEFINITIONS

ALL DEFINITIONS APPLICABLE TO MANNED FLIGHT ARE CONSIDERED TO BE EXTANT EXCEPT WHERE MODIFIED HERE.

2.2.2.1 UAV (Unmanned Air Vehicle, Unmanned Aerial Vehicle)

An air vehicle which is designed to operate with no human pilot onboard.

A cruise missile, ballistic missile, model aircraft and TBD are not considered as a UAV.

2.2.2.2 UAV System

The UAV system comprises all elements or subsystems necessary to command and control a UAV to achieve flight in accordance with specified operational objectives.

2.2.2.3 ROA (Remotely Operated Aircraft)

The US acronym for a UAV.

2.2.2.4 Remotely Piloted Vehicle (RPV)

A UAV that cannot operate in an autonomous or pre-programmed mode.

2.2.2.5 Unmanned Combat Air Vehicle (UCAV)

A UAV that has a mission designed for combat.

2.2.2.6 Ground Support Equipment (GSE)

All equipment needed to test, support and maintain the UAV system on the ground.

2.2.2.7 Control Station (CS)

A facility from which a UAV is controlled for all phases of flight. This may include the elements necessary for all phases of flight from take-off preparation to recovery, if applicable, that require system intervention and/or acknowledgement of system readiness.

2.2.2.8 UAV Data Link

The medium used to communicate between the UAV and the CS for command and control.
A communication channel between one or more Control Stations and one or more air vehicles, or between multiple air vehicles.

2.2.2.9 Emergency Procedures

The procedures used in conjunction with the Emergency System.The emergency procedure may be a “Flight Termination System” however this is a matter of system design not regulation.

2.2.2.10 Emergency System

The system designated to monitor, prevent and/or restrict an uncontrollable ongoing flight condition.

2.2.2.11 Autonomous

The execution of processes or missions using only on-board decision capabilities.

2.2.2.12 Airworthiness

The compliance with all applicable airworthiness requirements as specified by the State of Registration. This would normally comprise the Type Certification standards applied by the State of Design but can, and often does, include additional requirements specific to the State of Registry.
Airworthiness is therefore not a fixed concept, but the levels will vary from state to state. However all States must provide a minimum level of airworthiness as dictated by ICAO Annex 8.

2.2.2.13 UAV Commander

The person with the legal responsibility for the safe operation of the UAV System.

2.2.2.14 UAV Pilot

The person in direct control of the UAV.

2.3 SAFETY

2.3.1 Underpinning Safety

There is much work in progress in many forums such as the EU funded USICO programme looking at the safety issues related to UAV Systems and it would be premature to pre-empt this work within this document. Of significant interest is the need to recognise that safety is achieved through eddressing many issues related to the UAV System.

The four key areas underpinning Safety for UAVs as shown in Figure 6-2 and indeed for all aircraft are:

- Security
- Airworthiness and Certification
- Operations, maintenance and licensing
- Air Traffic Management

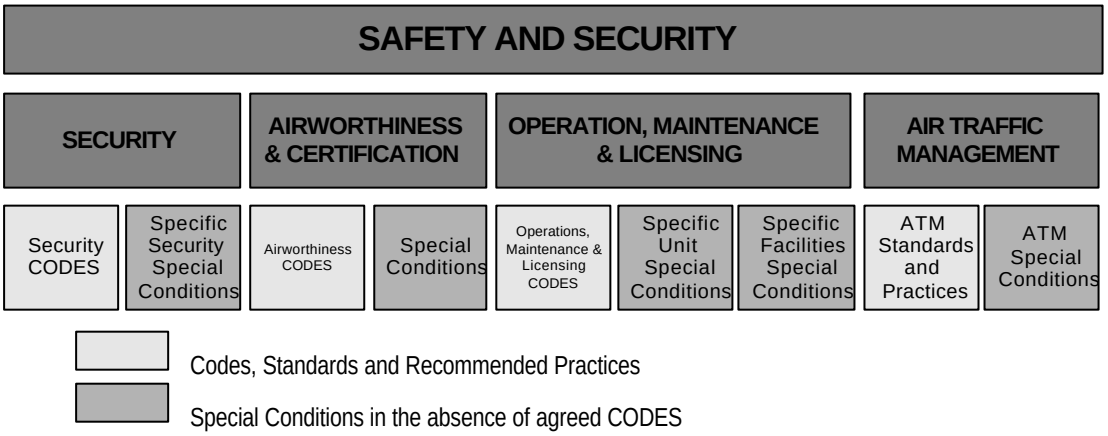


Figure 6-2 - Safety Priority, Supporting concepts and implementation aspects

These areas are addressed in the first instance through a combination of adherence to agreed Codes, Standards and Recommended Practices. Many of these have been developed over a number of years.

In the absence of such codes, the second approach, the second approach is to adopt a risk based approach in which structured arguments are used to articulate why certain special conditions contribute to the safety of a particular system. These arguments are usually encapsulated in what are termed safety cases. Figure 6-2 shows that the overall justification for the safety of a UAV System is built from both approaches and neither is exclusive.

Although Security is already addressed within Airworthiness and Certification, there are a significant number of issues that are not covered. For this reason Security is considered as a separate area. Paragraph 7.5 provides more detail on special conditions.

2.3.2 Goal Structured Notation

It is helpful sometimes to adopt some form of rigorous approach in the pursuit of determining that the system is fundamentally safe to be operated. Appendix 2 provides and example.

2.4 SECURITY

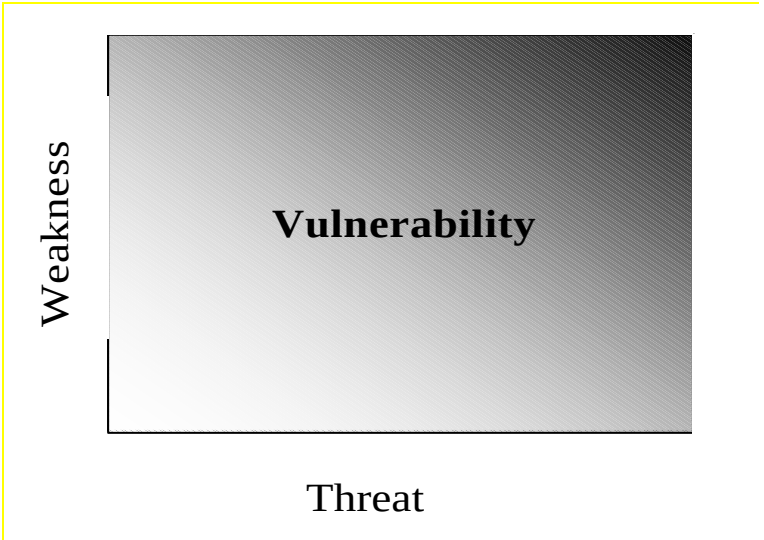
2.4.1 SECURITY OVERVIEW

This section explores the issues associated with security in relation to Unmanned Aerial Vehicle (UAV) systems. It discusses the aspects of security required to operate a UAV safely in all classes of airspace and forms the basis of a framework for future regulations. Initially each topic is introduced with a rationale for its inclusion and then expanded to provide the information necessary for the definition of the framework.

Within the overall topographical architecture this section addresses the system security aspects and the issues that emerge. In order to maintain a consistent security approach, from the splitting of the interface between the pilot and the air vehicle to communications with ATM and the subsequent control of the air vehicle, security factors have been treated at a system level.

The aim of this section is to provide an initial insight in to the security factors that need to be addressed if UAVs are to coexist with manned flight without special provision. Unlike many areas that are being addressed within the JAA/Eurocontrol Task Force where a direct mapping of the regulation associated with the manned world can be made, the un-manned world introduces issues of security that did not previously exist.

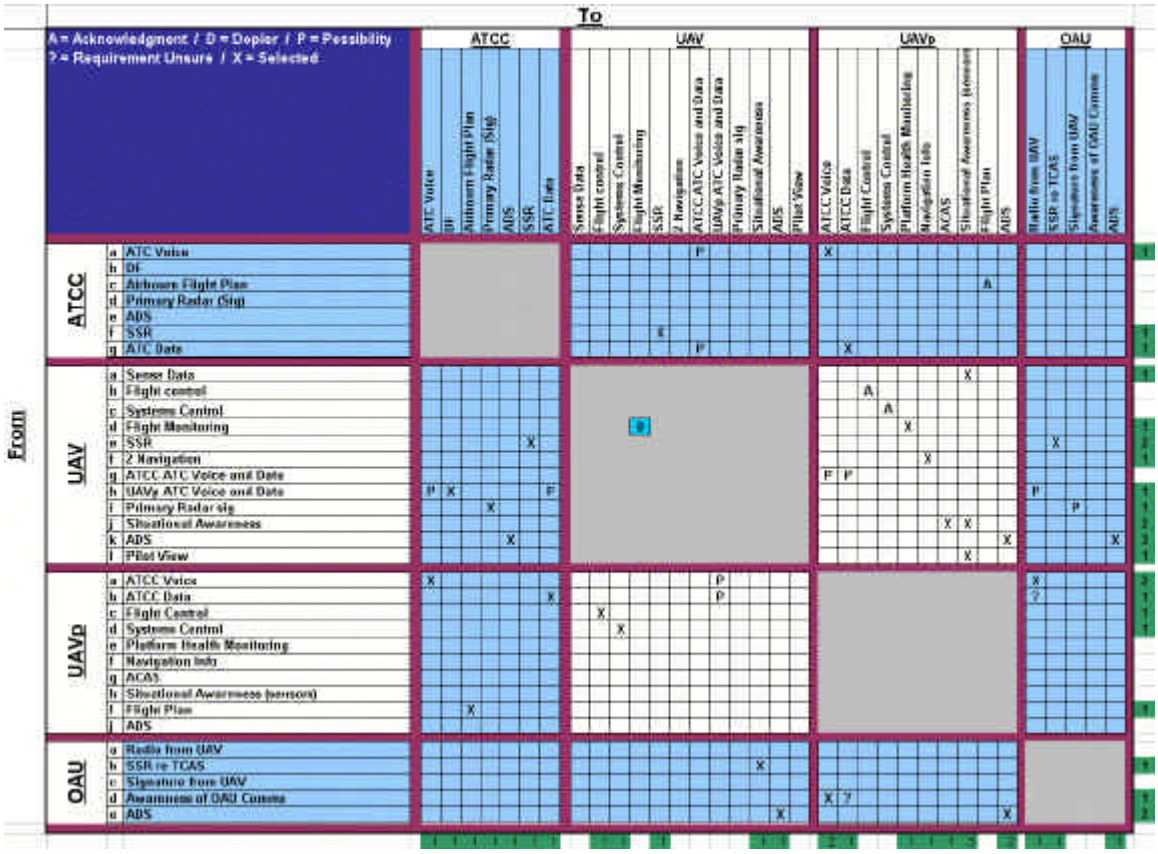
Security, is the balance between Threats and Weaknesses defining the system Vulnerability and determines the level of security measures that should be taken. The “Red” area, in the figure below represents, where there are large weaknesses and a high threat. Also a factor associated with security that must be addressed is the “desirability to an adversary”. If a system cannot provide any gain then it is unlikely that it will experience an adversary attack whereas a UAV with a high potential for damage or commercial advantage may attract considerably more attention and therefore the security measures necessary should reflect this. It is therefore clear that if desirability is considered a weakness then this is where the highest level of security is required. Conversely if there are no threats there is no need for security irrespective of the levels of weaknesses. It is from this that the Threat can be seen to have a direct correlation of the system Vulnerability.



Cost effective security is a balance of strong electrical and mechanical mechanisms to procedural measures. No one measure can protect against all the vulnerabilities and the strength of mechanism used will need to be chosen on a case by case basis. The following sections describe the approach recommended to lead the civil UAV system designer to a cost effective solution based on the air vehicle, mission capabilities and desirability of the system.

The issues associated with malicious and hoax ATC transmissions are the same as those for manned flight and even though the UAV pilot is not in the aircraft the dangers are the same. These therefore will not be covered here as they do not pose additional resultant risks because the introduction of UAVs.

It may appear that there is a difference between integrity of the data link and security of the data link but loss of one leads to loss of the other and therefore leaves the UAV open to safety issues. There are VHF, Satellite and Mode S data links presently used by manned aircraft and one topic for further investigation would be the issues presently being experienced with their use. However it should not be forgotten that the scenario for the UAV introduces many additional factors that are not present for manned aircraft. If a manned aircraft looses all external contact the pilot is still in direct control on the platform whereas the UAV may continue a pre-programmed flight path. The presence of emergency "Collision Avoidance Systems" does help with the overall safety of the system in this scenario. The figure below highlights the communications between multiple air users, ATC, the air vehicle and the UAV pilot (UAVp). The communication channels in the "Blue" signify communications channels that exist in manned aviation today and therefore may be utilised by UAV operations maintaining Transparency and Equivalence. The areas of communication highlighted in the two white boxes represent those that are specific, and new, to the UAV System. However it should be noted that not all the communication channels highlighted require security and the case for this should be explored in the Safety Case.



The work identifying the possible communications between ATC, UAV, UAVp and other air users was conducted by UAVS and can be found in full on www.uavs.org .

Within the principal of equivalence the ground to air communications should provide the same robustness as the control provided from a pilot in the aircraft.

Many of the issues in this section are not necessary for military UAVs as both the scenario and the airspace imply that the same stringent measures necessary for the co-existence of

commercial flights and UAVs will not be necessary and thus individual country military requirements are outside the scope of this section.

The design environment needs to maintain the necessary rigour to ensure that the design meets the required standards. This is presently the case for manned aircraft and equivalence means that this should be carried into the unmanned world. This is outside the scope of this section as it is covered within the activities of Section 3.

There are security issues associated with maintenance and development staff integrity and the malicious damage that could be caused. This is not directly related to the subject of this paper and will be covered within the Operation activities described in Section 4.

This paper has not attempted to deal with the handover from one control centre to another other than to state this as a requirement of Integrity, Access Control and Non-repudiation guidelines discussed later. Either a controller is authorised to control the Air Vehicle or they are not. The change of controlled area, UAVp or ATC centres should be a procedural measure as it is in the manned world today within the framework described.

The Security issues are related to the overall "Safety Case". Therefore within the Safety Case the need for Security will be ever present. Developed here are the guidelines necessary to explore and develop the underling levels of security required within a solution to meet the required Safety requirements. It is important that any regulatory framework provides a guideline and not a solution space. To this end a range of measures are described for each factor. Dependent upon an analysis of the Threat to the air vehicle, other air users, ground installations and the population at large matched against the desirability of the system to an adversary, a balanced set of security measures can be chosen to satisfy the vulnerability of the system through the safety requirements. However, it is recommended that if a particular factor is not implemented in a specific scenario the Safety Case should specifically justify its omission. This way "positive omission" can be ensured.

2.4.2 ASSUMPTIONS

The principle of transparency requires that Air Traffic Control (ATC) communicate with a UAV in exactly the same way as for a manned aircraft. If a UAV is to operate in all classes of airspace it is important that a range of security measures be defined that allows the many and varied damage potentials to be managed.

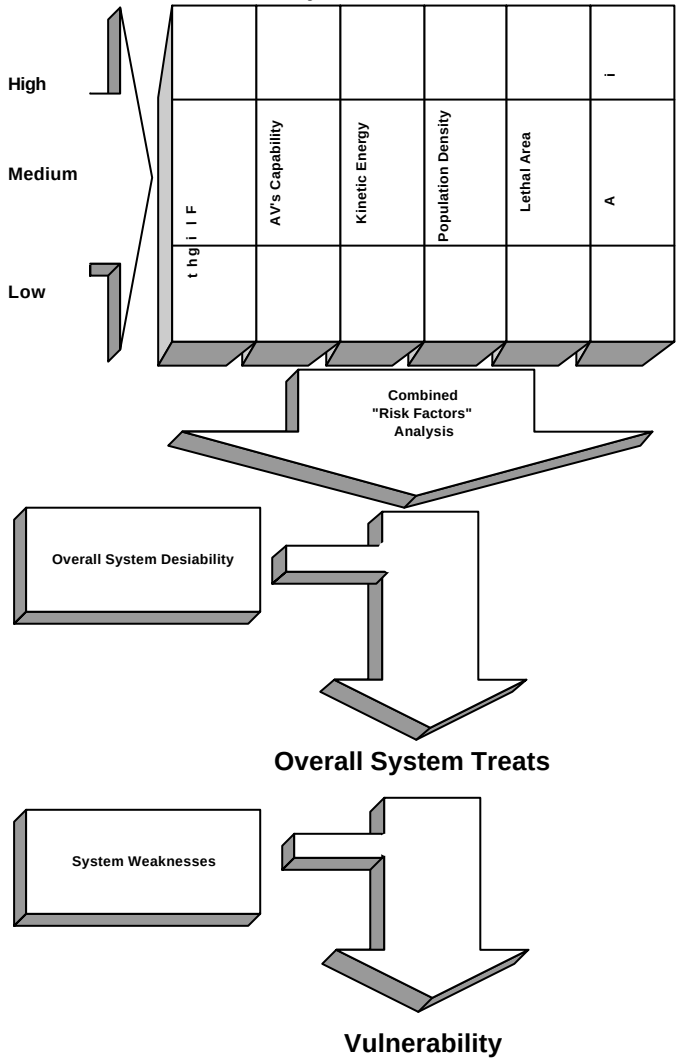
The measures/approaches identified here should not be driven by, but not preclude, the possibility for manned UAVs where the man is not the pilot.

The security issues and approaches described here will be driven from the Safety Case. All references to "Data Rates" and "Bandwidth" refer only to that necessary for safe flight and do not include any provision for payload as this is a commercial and not a regulatory issue.

2.4.3 THREAT ANALYSIS

The security measures that can be applied to the Data Link, Data Network, Processing Unit and the Physical UAV pilot (UAVp) vary considerably dependant upon the Threats that could be posed by and to the UAV system. It is therefore imperative that the market for UAV systems is not constrained by security measures that are not appropriate to the specific characteristics of the air vehicle, system or mission. It is equally important that the security measures are sufficient to support the required safety levels and that security is not reduced creating an unsafe environment. The view of Vulnerability described earlier emphasises that there is not a prescriptive set of security measures that apply to a particular air vehicle of operational air space.
A framework driven from the Threat Analysis of the flight profile and the potential for damage is seen as the best approach. An example is a Large UAV operating over the North

Atlantic with a range of 50Km poses a low risk to life resulting from "Unlawful Intervention" as it does not have the capability to over fly populated areas, oil rigs etc.[1]. However a UAV operating over a large city, would pose a serious potential for damage if "unlawfully intervened" with even if its size and energy is considerably less than the UAV in the first case. In the second case it is clear that measures taken to protect the system should reflect this increased threat, being careful not to impose unnecessary costs and operational constraints where unnecessary. However the potential for damage is consistent with the Kinetic Energy, Intended Airspace, Lethal Area, Flight Rules, the Air Vehicle Capabilities and Population Density over the complete flight track. Much of this work has been conducted with respect to examining the categorisation of UAVs. Whereas categorisation for categorisations sake may not move the security of commercial UAVs forward little, the topics provide a good standard way of defining the factors and their importance in the context of Threat Analysis.
It is from this that all the top-level requirements for security can be drawn. However, it is important to remember that the damage to be considered is not confined to the impact created by the UAV on the ground but to any other manned or unmanned aerial vehicle. Therefore elements of the threat analysis need to address this.



The Threat Analysis should take into account the possible damage to public confidence in UAVs resulting from an occurrence. This security section only concerns itself with those issues through Threat Analysis and the resulting Vulnerability that determines the Security measures applicable to a UAV and/or its mission. There is a similar concern with respect to

[1] In the example it is assumed that the characteristics of the air vehicle with the UAV launch area position, does not allow flight within range of any fixed installation, land fall, major shipping lanes etc. and therefore the potential for damage is limited.

the severity and probability issues concerned with safety. The boundary between Security and Safety becomes blurred as the security measures are designed to maintain the safety of the system. As we are not concerned with the payload issues here, if there were no safety issues then the Threat Analysis would be low and therefore very little provision for Security would be necessary.
Although this does not maintain the principle of equivalence and should not drive the underlying minimum requirements best practice should take cognisance of the public perception.
It should not be overlooked that Physical Security measures are dependant upon the results of the Threat and Vulnerability Analysis and the Operator's system solution should be included in the Safety Case with full justification of the system solution provided.

2.4.4 SECURITY FACTORS TO BE CONSIDERED

This section introduces the top level of the topics to be considered in any proposed security framework designed to meet the requirements of a Threat Analysis. UAV Security breaks down into :

- Physical
- Data Links
- Data Networks
- Software

It is not considered that Hardware security needs to be explored in this context as the airworthiness certification of the system should protect against attacks, failure and/or fault tolerance risks of this nature. The other subjects will be covered in turn. Notwithstanding this, the development environment should be maintained at best industry practice and thus the risks to the individual hardware and software designs elements should be apportioned design criteria and result in the design and evaluation rigor necessary. The underlying requirement is for the System Security to provide the necessary protection to the level determined by the Threat Analysis. The hardware/software split necessary to provide this becomes an issue for implementation and not for regulation[2].
The security measures here examine the core differences between piloted and unpiloted flight:
The availability of the pilot on the ground,
The need for defendable occurrence investigation data,
The access to UAV control data by a third party,
The impersonation of the UAVp by a third party,
Intentional data link disruption,
Correctness of data transmission
UAVp ground station access control

2.4.4.1 Physical Security

The confines of an Aircraft and the pre-boarding checks make the takeover of a plane, notwithstanding the events of September 11, difficult. An adversary can only have with him/them what can pass though the modern security checks. Whereas a ground based attack could have unlimited manpower with weapons of choice. It is therefore clear that the threats and vulnerabilities to a ground-based pilot are the same (why the same – argument says that the threats to the UAVp are greater than those of a normal pilot), if not greater, than those of a pilot in a manned environment.
It is therefore clear that a minimum set of security guidelines need to be drawn up if the UAVp is to control an aeroplane in controlled airspace and that the minimum level of physical security must be driven for the threats and vulnerability of the system. Although a ground based UAVp poses different security issues it does have the advantage of allowing

[2] Hardware certification may be necessary for the highest levels of Security and this can be conducted through National accreditation means that already exist.

multiple sites to be used. This is not attempting to say that access to an Area Control Centre is easy but that the UAVp must be protected.
The initial assumption of ATC transparency does not necessarily mean that the UAVp be co-located within ATC broadcast range as data networks allow the UAVp to be located anywhere with voice commands digitised and transported to him and outbound commands networked and broadcast to the UAV. A networked system would provide the same level of transparency to the ATC Controller as in manned flight[3]. This allows the levels of security necessary to protect the UAVp to be placed where it can be best provided. It is clear that the focus on Physical Security is not a prime driver for this framework, however in providing a complete regulatory framework this should not be forgotten and the appropriate levels determined based upon the Threat.
The specific Physical Security levels necessary should be defined by a clear "Threat Analysis Process" enabling clear rules to be determined. Dependant upon the "Threat Analysis" the UAVp could be anywhere from "open land" to "high security". The regulatory framework should allow the necessary flexibility and security without constraining operator solution design.

2.4.4.2 Data Link Security and Integrity

There are a number of topics that should be addressed within a commercial UAV System by either inclusion or specific exclusion in the safety case. However the levels of each factor applied to a particular system will be dependant on the Threats and Vulnerabilities identified earlier. A justification for the levels chosen for each factor should be provided in the Safety Case.

Resilience

Resilience is the measure of the systems inherent survivability faced with a security attack. The security, operational and procedural measures combine here to define the overall system performance[4]. As Vulnerability is the combination of the Threats and Weaknesses the System Resilience must be equal to the Vulnerability.

Bandwidth and Data Rate

The data rate and bandwidth necessary to support the UAV C2 system will have a bearing on the type of security provided at each threat level. This is caused because of the variations of mechanisms available and their suitability to particular data throughput. Inherently there is a high probability that the security mechanisms deployed in to a particular system will add data to the channel. Therefore the bandwidth available compared with the solution system control bandwidth may dictate the type of protection that can be employed. This is not saying that one mechanism is stronger or weaker than another only that the available bandwidth is an important factor in choosing the final system configuration[5].

Anti-Jam characteristics

Dependant upon the threats and vulnerabilities associated with the specific characteristics of the UAV and mission profile this will range from the need for no measures to be taken to full state of the art protection systems.
However for systems that provide situational awareness, independent "Sense and Avoid" and provide emergency avoid action it will be found that the consequences of jamming will have

[3] See the Data Network Security section below.
[4] An example of resilience could be; an attacker gains access to the air vehicle control through the data link and instructs it to "dive" in to the ground. However the command is outside the flight envelope and the procedural interlocks to operate outside that envelope are not followed, so the air vehicle continues on its original flight path. This allows the authorised UAVp to regain control. In this case there would be a level of resilience provided by the UAV System greater than that of the individual elements.
[5] The provision of Spectrum for Commercial UAV Systems has been added to the agenda of the 2007 World Radio Conference (WRC 2007)

less impact on safety than on a system controlled directly from the ground via a UAVp. Notwithstanding the above anti-jam characteristics could have a major factor upon mission success. It should not be forgotten that a UAV system being jammed may not pose an immediate hazard. However not being under command, and dependant upon the operational environment, the UAV may have a pre-programmed flight path and will have an "Emergency procedure" thus an immediate danger may not exist.
The loss of the data link for more than a predetermined time or the loss of the data link in a specific geographical area may cause considerable safety hazards and the underlying severity of these will be dependant upon the Threat Analysis conducted. The Threat Analysis will take into effect the air vehicle characteristics, flight path, desirability, data link loss procedures etc. and thus the case will be different for each air vehicle.
The Anti-Jam characteristics applied between particular air vehicle and its ground station will be consistent with those necessary to meet the operational analysis of Vulnerabilities and justified in the Safety Case.

Maximum drop out and UAV Actions

If the communications link "drops" for greater than a specified time, based upon the Threat to the UAV, the UAV must be considered to be "not under command" and therefore specific actions should be taken to alert other airspace users. Depending on the threat, and the necessity to maintain communications, it may be necessary to initiate existing manned procedures and secondary systems that communicate to other airspace users if the primary control is not available if the Data Link is lost. This applies to either loss of the data link as well as the jammed data link.
In Manned Aircraft, if the carrier link is lost for more than 3 seconds then the ATC voice link is considered to have been lost from that point until it is re-established. The case of the UAV is different from that of manned flight in that the Pilot is not in the Aircraft. In manned flight although communications is lost, safety is preserved. With a UAV the pilot is in control through the data link and therefore the constraints on link performance are different.
There are many techniques that can preserve a "Data Link" through a variety of harsh environments and the degree that these are employed, within a particular UAV system, will be dependant upon the Vulnerabilities identified for that UAV system.

Non-repudiation

A scenario unique to the UAV is that in the event of an accident the pilot will inevitability survive that incident. Thus the UAV System must collect all evidence of action and reaction in a non-repudiated way worthy of court examination. Whereas at first this does not appear to be a security issue it must be made clear that collection of data of this type and "end use" requires the highest levels of design rigor that is usually only found in the security of safety critical technology areas. It must be possible to analyse who sent a command to the UAV and when. Non-repudiation will allow the sender of the message to be clearly and accurately determined such that the source cannot repudiate it.
This should be extended to "two-way" repudiation providing evidence that the correct UAV received, and confirmed, the transmission and responded in line with the confirmed delivery protocol.
This does not necessarily apply to ATC in this instance but this too should be recorded. The main thrust is that the UAVp who sent a command to the air vehicle that caused the incident should be identified though a non-repudiatable mechanism admissible in a court.
The levels of non-repudiation necessary in a particular application will depend upon the Threat analysis conducted.

Protocol Characteristics

There are a number of characteristics that will be needed in the communication channel between the UAV and The UAVp, these include defined Command, Action and Reaction data

flows. This should be designed such that the data transmission, or not, can be proven. This is linked to the requirement for non-repudiation in that the proof of command transmission and receipt may be needed in court and data may need to be recorded by both ends. This is analogous to recording the pilot actions in the cockpit of a manned air vehicle today. In the limit the flight end of a link may need to protect the data stored with "anti-tamper" mechanisms applied to prevent post incident alteration. The transmission protocol should allow both ends to determine that the message has been received as transmitted.
There are a number of protocols, both technical and procedural, that have both resilience to and recovery from collision. However the protocol necessary for a given scenario would be dependant upon the Threat Analysis. This is also dependant upon the latency that can be tolerated.
Although initially many of these characteristics may not seem like security issues, weaknesses in this area can provide an opportunity for a denial of service attack that could render the UAVp helpless.
The main features of a communication channel characteristics discussed are therefore:

- Defined command, action and reaction data flows between the UAVp the UAV and ATC
- Transmission collision
- On board recording
- Commands and responses
- Information and acknowledgement
- Timeliness
  (important in congested airspace – the protocol must support multiple UAVs and UAVps without degradation on performance and the baseline performance must be appropriate for control of the UAV).

The extent that any of these mechanisms are included in a particular design or mission fit is dependent upon the Vulnerabilities identified from the Threat Analysis. A justification that the mechanisms employed within a particular design should be provided in the Safety Case. There are a number of protocols in use today that provide this level of information assurance and the use of these should be explored.

Authentication

The UAVp will inevitably be isolated from the UAV by a data link. However the UAV needs to know that the command received has been sent from a person authorised to provide control data. This is in essence different from "unlawful intervention" in that the command may come from the correct ground station. It is therefore clear that in many cases the Threat Analysis will show that a lack of authenticated UAVp identity is a Vulnerability. The UAVp will therefore need in many cases to Authenticate themselves to the workstation and an authentication code sent to the UAV for recording of a commands origin. The validation of a UAVp must utilise two factors. This means that it should rely on a minimum of two of the factors listed below.

- Something you know
- Something you have
- Something you are.

Reliability

The reliability issues should be dealt with under Air-worthiness and are examined in Section 3. However the security implications associated with a lack of reliability should not be forgotten. This is an important aspect of the mechanisms employed – if a security mechanism fails then it could result in denial of service – it seems that the "Security Case" and "Safety Case" are intimately related.

Integrity

The integrity of a system can be measured in many ways but is fundamentally associated with the correctness of data – whether the incorrectness of data comes from error or malicious alteration. The ability of a UAV System to carry out the commands given by the UAVp, applicable to a UAV, or the ability of the UAV System to maintain its environment. It is clear that the UAV System must carry out the instruction provided by the UAVp in an assured way. There are a number of standards associated with Integrity and the certification process is not trivial. However dependent upon the Threat Analysis results the level of integrity required by a system will vary greatly. It is fair to say that a UAV over a populated area with high damage potential should attract an integrity requirement whereas the UAV example used over the North Atlantic may not irrespective of its energy potential.

2.4.4.3 ENCRYPTION

It is believed that "encryption" needs to be in a different section as this is a Security Feature that may or may not be needed –it can be used to provide protection against several different vulnerabilities. The feeling gained from this paper to here is that the potential weaknesses are identified rather than the specific mechanisms used to mitigate against these weaknesses. Encryption can benefit the safety of the UAV design in a number of ways. Based on the Threat Analysis, and the balance of other mechanisms employed, encryption can provide a number of advantages to the UAV System Designer. The main benefits of utilising this technique are:

Protection from eavesdropping on UAV C&C2 channel could, and in some cases should, be protected through the use of Encryption if identified as a mitigation strategy to a Vulnerability.

This in itself does not, assuming non-repudiation, provide protection from Unlawful Intervention. However encryption does provide an added protection. In fact, with proper management, this should be the strongest mechanism in this regard providing:

Protection from Eavesdropping on control data communications why a problem?,

Non-repudiation between the Ground Control Station and the Air Vehicle[6] [7]

Protection from "Unlawful Intervention", see Footnote 7.

Air vehicle differentiation, see footnote 7.

Encryption on its own does not provide any evidence for an investigation however correctly decrypted data does stand to provide a proof of source that could be admissible.

ATC is conducted on open frequencies and thus this type of protection is more aligned to UAVp to UAV communications.

The inclusion of encryption and the level and rigor it is employed will be dependent upon the results of the Threats Analysis and the determined Vulnerabilities of the system.

2.4.4.4 DATA NETWORK SECURITY

There are a number of scenarios where operation over a data network could provide the best UAV System solution. However what needs to be agreed is the integrity, robustness and timeliness of the communications between ATC and UAVp. This is not constrained to data networks. Thus whatever the transport mechanism is, it must meet the security criteria to achieve equivalence. If an operator chooses a data network then the mechanisms employed must meet the criteria laid down. An example is GSM encryption over the air, this affords the user the same level of confidentiality as that of a landline and that's all. Therefore security of both ATC and C2 data transmitted over that network needs to be addressed. The advantages of this approach are many and varied ranging from transmission of control data to a central point facilitating the secure location of a UAVp and transmitting ATC voice from any international flight area to the UAVp.

[6] This does not provide authentication of the Pilot to the Ground System.

[7] This is only possible with careful Key Management. Open access to the Key Data would render encryption transparent.

It is therefore imperative that data used on a network be protected from modification and interception. The primary means for this would be "End to End" encryption services with the strength mechanism being dependant upon the outcome of the Threat analysis.
However notwithstanding this the variety of mechanisms available affords varying levels of security and it is envisaged that operators will continually utilise the maximum strength mechanism they have. Therefore the operators and manufactures would use the Threat Analysis differently here from the other factors described above. The Operator/Manufacturer would choose the mechanism strength, as the minimum mechanism strength necessary to achieve the maximum threat the particular Operator/Manufacturer envisages being in control of. The algorithm strength necessary may also be determined but the National Agencies in collaboration across Europe.
It is important here not to just think of the network as a closed system. An end-to-end encryption system approaches this but if an alternative network security topology was chosen the Architecture would need certification against the security targets resulting from the Threat Analysis. Each Nation has a security evaluation agency and they should assess the underlying strengths and their in-country implementation.
Where it may be considered that networks are non-deterministic and that timely delivery and assured secure routing may cause problems, the effects of these are all factors of network design in modern systems. There are many ways the network could be configured which would be dependant upon the Threat Analysis. The acceptable level of latency in the specific situation will be a driver on the network configuration and topology used as this can be varied considerably by design.

2.4.4.5 SOFTWARE SECURITY

This section covers the aspects of security that are associated with the software. It is important to note that the security of the UAV System should address the software in both the Air Vehicle and Ground Station.
This may need to be to the same or greater rigger than that for manned. As there is no pilot to deal with the vagaries of the flight profile. History has shown that only the most rigorous software development cycle and evaluation to the levels described in ITSEC documentation can be trusted. However full evaluation to the levels in ITSEC can be costly and therefore the correct level should be chosen associated with the relevant Threat Analysis.
Where a common evaluation methodology is used for more than one factor the higher evaluation level resultant from the Threat analysis should be used.

Software Upload

It is becoming regular practice to upload software prior to the mission allowing the characteristics of the vehicle to be "trimmed" to the mission profile. This approach is being further developed by the JSF programme and therefore within the life of any regulation may become common place across all platforms. It is therefore imperative that any future regulatory framework addresses this ensuring that the performance and characteristics provided are those that were intended and that the information uploaded is received unaltered. Precautions here are clearly necessary
The purpose of this paper is to identify the measures that should be considered and developed for a regulatory framework. It is therefore suggested that the burden of proof that a proposed UAV System, and the mechanisms it employs, meet the requirement as outlined by the Threat Analysis lies with the Manufacturer and/or Operator. Notwithstanding this it is recommended that techniques such as cryptographically binding the operational code, data integrity checks etc. should be examined.

Malicious Code Prevention

With safety of prime concern and the proliferation of software driven systems, the ability for software programmes to contain "Trojan Horse", code that only runs on a certain date or set of circumstances designed for destructive purposes, is increased. Again there are degrees of analysis that are defined in the ITSEC Criteria that would find such code. However, as before, the level of ITSEC evaluation necessary for a given system should be determined by the Threat Analysis and the assessment of te system Vulnerabilities.

Development Integrity

There is a clear need to be sure that the code is evaluated to a level consistent with the Threat Analysis. Airbus attempted to over come the high threat posed by having multiplication of systems developed by independent teams. This approach only works if each team uses different Languages, Compiler Manufactures, Design Philosophies, etc.. This is not necessarily being proposed for the UAV system but merely shows that this is a real threat to the Safety and Security of a UAV system and solutions have been devised to over come them. It is clear that the Airbus solution may be over the top for most UAV system but the correct level of development integrity designed to meet the Threats should be determined.
In most cases software development and evaluation standards as identified in the ITSEC criteria[8], accepted throughout Europe and the US, would be sufficient. However the levels of design rigour and evaluation defined in the ITSEC criteria would need to be mapped to the Threat Analysis so as not to unduly burden UAV Development costs where the Threat does not require it. It is not intended that these measures impose any more constraints than those that exist in the manned world for similar air vehicles and a similar mission profile.

2.4.5 TERMS AND DEFINITIONS

This section attempts to provide a clear definition of some of the terms used in order to aid the reader..

To repudiate	To deny that information is correct casting doubt on it's authenticity. This is often used in conjunction with evidence used in court.
Non-repudiation	This is used to define the mechanisms incorporated to remove doubt on the authenticity of data. Therefore the mechanisms used must in themselves be "trusted". Use of this type of mechanism means that both sides will agree that evidence submitted is correctly collected.
Unlawful intervention	This term is used to describe where an unauthorised party takes or disturbs control of a UAV or Ground Station without the permission of the UAV Commander. In this case the intervention is assumed to be malicious.

[8] I'm not sure ITSEC would be applicable – it may be more applicable to use the methods imposed by the aircraft industry today regarding the development of flight critical or flight safety involved software. ITSEC isn't really geared up to evaluate avionics control systems – however if you are creating a ground-based authentication system for UAVps to logon to then ITSEC is applicable.

2.5 COMMUNICATIONS, COMMAND AND CONTROL

This section has been included in the document for completeness but is not part of any regulatory framework. The framework discusses the provision of a safe UAV system through the use of a Safety Case underpinned by the extant regulations and specific mitigation strategies applied to the risks identified. The Airworthiness and Certification, Operations and Security sections provide techniques and tools to aid with that risk mitigation process.

Communications, Command and Control become an application that operates within the safe system provided. The data link, its integrity, the control station and response of the air vehicle are all catered for within the Safety Case environment proposed. Therefore the Communications, Command and Control aspects are covered within the provisions of Sections 2, 3 and 4.

The UK DAP has proposed that the provision of radio frequencies UAVs be investigated by the World Radio Conference and this has been accepted on to the agenda for 2007. This is an important step in moving towards conformance for UAVs world wide and should be supported.
