The Swedish Aviation Safety
Authority

Flying with unmanned aircraft (UAVs) in airspace involving civil aviation activity

Air safety and the approvals procedure

(English translation of “*Flygning med obemannade luftfartyg (UAV) i luftrum med civil flygverksamhet*” avilable at www.luftfartsinspektionen.lfv.se)

Produced by Eskil Wiklund

Approved
Norrköping, 25 March, 2003

Arne Axelsson
Aviation Safety Director

CONTENTS

1. BACKGROUND

Unmanned aircraft are currently referred to as *unmanned aerial vehicles, uninhabited aerial vehicles* or *unmanned air vehicles*, for which the acronym is UAV. They used to be called RPVs, *remotely piloted vehicles*, a common designation for unmanned aircraft.

Model aircraft are not normally referred to as UAVs and are not inspected by the Swedish Aviation Safety Authority if they weigh 12 kg or less (although no such weight limit has been officially established) and flown exclusively as a hobby.

A number of UAV projects are in progress in Sweden, some of which are well advanced.
Approvals for flight testing and operation have already been granted for some civil projects. Applications for military UAVs to be permitted to fly in airspace where civil aviation occurs are expected shortly.

An agreement between the Aviation Safety Authority and their military counterpart FLYGI has been reached concerning co-operation on matters of air safety within the sphere of UAVs. A common policy document is in preparation. Collaboration on classification is currently in progress, with five different classes having been defined.

Civil and military regulations for UAVs and UAV systems are both currently lacking in most countries, including Sweden. Regulations are currently in preparation within JAA with Swedish participation. This is normally a comparatively long drawn-out process. This advisory document has been developed in order to allow UAV flying in Swedish airspace where civil aviation activity is permitted before international provisions have been worked out and established. The document emanates from a principle that comprehensive air safety objectives should be fulfilled for all UAV systems collectively.

This document lays the stress on the design of a UAV system, but some advice is also given as regards operation. The Aviation Safety Authority has commenced working on an advisory document which deals mainly with operational matters.

In order to facilitate the development of UAV systems in the initial phase, considerations has been taken to ensure that the number of UAVs flying is small thus limiting the number of accidents. This will ensure that the overall risk to people on the ground is low as will be the risk to those onboard manned aircraft. This will initially allow a relatively high accident risk per flight within a UAV system, but the risk must be strongly reduced with increased flying time. With an increasing number of operators the permitted accident risk (calculated per flight hour or per flight) must also be reduced.

What the international regulations for UAVs will contain is not yet known. They will probably contain some elements of special design regulations for the craft themselves and other technical equipment, in conformity with JAR-VLA or JAR-23 in applicable extent and with certain additional requirements, e.g. for links and operating stations. In addition, it is likely that special operational and training requirements for "pilots" and system operators will be developed.

2. COMPREHENSIVE AIR SAFETY OBJECTIVES FOR UAV SYSTEMS INTENDED FOR OPERATION WHERE CIVIL AVIATION ACTIVITY OCCURS

The Swedish parliamentary act of 1987/88 concerning air traffic stipulates that Swedish air safety standards shall be on a par with those in other well-developed aviation nations. How this objective is to be achieved and measured is left to the Aviation Safety Authority to decide.

In 1998, the Government set a target that the number of accidents per flight hour in Swedish licensed air traffic and the number of accidents per year within Swedish private aviation shall be halved by the year 2008.

The above objectives only relate to those onboard. No objectives have been set up concerning the risk to persons on the ground. However, reasonable probabilities for persons on the ground are achieved indirectly if the requirements for persons on board are fulfilled.

It is therefore reasonable to set objectives for UAV activity as regards the risk to persons on the ground (third parties), despite the fact that the Parliament and the Government have not specified any objectives for the corresponding risk involving manned aircraft. In addition, manned aircraft must be protected.
The Authority considers it reasonable that:

- it shall be highly improbable that persons on the ground should die as a result of crashing UAVs, even over an extended period of time. A maximum of one death per 50-year period can be permitted during times of peace;
- the personal risk to persons on the ground due to crashing UAVs shall be significantly lower than average personal risk in road traffic. A risk at least one hundred times lower should be striven for, since the risk is involuntary;
- UAV systems shall not give rise to more near collisions, calculated per flight (or flight hour) than what manned aircraft have caused during the most recent ten-year period. This applies especially if the other aircraft in such an event is manned. This shall apply both inside and outside controlled airspace.

Analyses showing that the requirements posed by the Aviation Safety Authority are being fulfilled must be produced before approval is given.

Section 3 discusses the requirements in greater detail and gives advice on how to demonstrate that the requirements are being fulfilled.

3. GENERAL ON FLIGHT SAFETY OBJECTIVES AND HOW FULFILMENT OF REQUIREMENTS CAN BE DEMONSTRATED.

No UAV systems have been designed or approved so far in Sweden with the aid of safety analyses. The Authority therefore considers it a matter of urgency for a dialogue to be set up between the Authority on the one hand and various applicants and manufacturers on the other, to ensure that flight safety objectives are expressed in such a manner that they are of assistance to designers and those appointed to scrutinize the systems from a safety point of view. Such a dialogue can also lead to a review of objectives or other types of objective when justified.

/Page 5/

Section 2 sets out the comprehensive air safety objectives for UAV systems in Sweden. It is however a major task to carry out analyses showing that objectives have been or are being fulfilled. All analyses are therefore marred by considerable uncertainty. It is thus not justified to require comprehensive analyses for less comprehensive systems involving minor risk to the environment.

The Aviation Safety Authority has decided, for example, that if the operator maintains continual visual contact with a small UAV in the immediate vicinity (e.g. in aerial photography) a relatively simple analysis will suffice. The analysis should show that the applicant has thought through the risks involved and that he has taken steps to eliminate or minimise such risks. Such an analysis will be entirely qualitative.

Special (occasional) solutions to compensate for faults or uncertainty in a UAV system may in some cases be necessary. A manned escort plane can be such a solution when the need to see other aircraft is essential and cannot be fulfilled. Until sufficient positive experience of a UAV system has been acquired, special air traffic controllers could be "lended" during the initial phase who will devote themselves principally to separating UAVs from other traffic within controlled airspace and to co-ordinate UAV flight paths with other ATS units.

An air traffic controller is expected to be able to fulfil the requirements he is qualified to perform. He is allowed to compensate for failure conditions, for which satisfactory warnings have been given, to the extent possible. To this end it is necessary, as in the case of a pilot, that an air traffic controller can carry out the necessary compensatory measures without exceptional skill being necessary.

The requirements on those operating a UAV can on the other hand be allowed to vary depending on the type of UAV and the operating conditions otherwise. However, exceptional skill must never be assumed in the analyses.

The content of what is expected of a comprehensive analysis is given below.

3.1 Safety analyses of heavy aircraft as a norm for UAV analyses

The term *failure condition* is used in FAR/JAR 25.1309 and AMJ 25.1309 for heavy aircraft or transport aircraft and FAR/JAR 23.1309 and AC 23.1309 respectively for light aircraft. It indicates the failure condition at aircraft level arising due to failure occurring at lower levels (e.g. maximum elevator deflection due to various technical faults).

The corresponding failure conditions in UAV systems (at aircraft level) shall be defined and investigated if they could involve serious accidents and near collisions. All types of serious failure conditions should be dealt with, irrespective of whether they are caused by hard- or software errors or an erroneous decision at operator level. Information which is difficult to interpret, extremely delayed or misleading to the operator should also be taken into account, as should the obvious risk for confusion of switches, buttons or such like. Knowledge of human factors should also be applied here.

AMJ up to 25.1309 (JAA Advisory Material Joint) and AC 23.1309 (FAA Advisory Circular) state the probabilities per flight hour which are permitted for failure conditions leading to consequences of varying degrees of gravity. To give an example, a failure condition involving disaster must not happen more than once every billion flight hours (10^9) for a heavy aeroplane, rising to once every million (10^6) for a single-engined, piston-driven aeroplane with a maximum starting weight of under 6,000 pounds. For intermediate categories, 10^8 and 10^7 apply.

/Page 6/

An underlying assumption is that fewer than 100 such failure conditions will normally arise in a heavy aeroplane, which means that the total probability of a disaster due to a fault on any of the aeroplane's systems should be less than one in 10 million (10^7) flight hours. Since the total number of crashes involving death (all causes) is also around one for every 10^7 flight hours for modern aircraft, this means that the design requirements have been well fulfilled as regards system faults. For a light aircraft with a maximum starting weight of under 6,000 pounds it is assumed instead that no more than 10 failure conditions exist which can give rise to a disaster, which means that system faults involving a fatal accident must not occur not more than once in 10^5 flight hours.

The Aviation Safety Authority proposes that AMJ 25.1309 and AC 23.1309 shall constitute the norm for proposed safety analyses of UAV systems. It is only the mode of procedure which is being proposed for application in the initial stage and not necessarily the strict requirements. A suitable mode of procedure could thus be to divide the total permitted probability into smaller parts. If, for example, the permitted probability is 10^{-3} per flight or flight hour due to the operating area and other factors and the number of failure conditions involving an accident is not more than 10, each individual failure condition may have a probability of 10^{-4}. Uneven distribution of the various failure conditions, if they still give a final result of maximum 10^{-3} can also be permitted. An advantage of an even distribution of probability is that designers of different subsystems can base their work on the same probability requirements for each subsystem at an early stage.

3.2 Attempts to calculate permitted probabilities for failure conditions involving possible injury to persons on the ground

The probability of someone dying in a road accident during a period of 80 years is around one in 250. The requirement for a hundred times lower individual probability due to a crashing UAV means that the individual probability must be not more than one in 25,000 during a period of equal duration.

As far as individual risks are concerned, population density plays no part in the same risk of crashing. For an individual person being overflown by a UAV it makes no difference if he lives in a sparsely or a densely populated area, provided the UAVs are the same and are operated in like manner over the areas concerned.

To limit the number of deaths on the ground however, the UAVs should - until they can demonstrate equally low probability of accidents corresponding manned aircraft - fly over unpopulated and sparsely populated areas.

The document *Suggested Flight Approval Process for Unmanned Air Vehicles (UAVs)* published by AeroVations Associates, gives the following formula (modified) to calculate the number of deaths on the ground where population density is an essential factor:

where $n_{fatality} = p_{c/f} \text{ x } (A_{lethal} \text{ x } d_{population})$

$n_{fatality}$ -is the number of fatalities (modified from the reference text's $p_{fatality}$ = probability of a single fatality) resulting from a crash, per flight hour

$p_{c/f}$ - is the probability of a "crash-inducing" failure, resulting in an uncontrolled crash of the UAV, per flight hour

$d_{population}$ - is the population density of the area at the crash site; and

A_{lethal} - is the area of the "lethal swath" of the crashing aircraft, that is the area at the crash location within which by-standers would suffer fatal injuries.

/Page 7/

The formula does not distinguish between persons indoors or outdoors. Generally speaking buildings and forests reduce the risk to persons on the ground in the crash location, especially for smaller UAVs with relatively low energy. The fact that persons are inside a building can naturally mean in individual cases that more people are hurt than would otherwise have been the case. However, the formula is statistically regarded as conservative and should be usable in an analysis.

All those struck by a UAV are presumed to die.

It should be relatively easy to produce $d_{population}$ for a large area, including dense population centres. If it can be shown that a UAV's flight can be controlled so as to avoid the dense population centres in this large area during normal flying and a crash area can be chosen in a sparsely populated area, it should be possible to calculate a lower $d_{population}$.

It is suggested that A_{lethal} be based on the most probable crash mode. If a UAV normally crashes vertically, A_{lethal} will be proportional to the UAV's exposure area and mass. Bearing in mind a flying object, a reasonable safety area should be assumed, with a size which is dependent on the crash energy and the probability and energy of components flung out, e.g. a rotor blade. For a UAV which hits the ground in calm weather at low speed in a functioning parachute no safety area need be assumed. For a UAV whose most probable crash mode includes a horizontal movement, a larger A_{lethal} should be assumed, whereupon consideration should also be taken to kinetic energy.

Multiplying the number of flight hours over 50 years gives the expected number of deaths during this period.
The formula is thus:

number of dead = $n_{fatalitytot} = p_{c/f} \times A_{lethal} \times d_{population} \times fh50$ (number of flight hours over 50 years)

It remains to calculate the permitted $p_{c/f}$ based on the other factors in the formula. $p_{c/f}$ is the sum of the probabilities for all failure conditions which can cause a crash.

The number of deaths is allowed to be = 1

The other factors depend on the circumstances prevailing. An example is given below:

$d_{population} = 1$ person/km²

$A_{lethal} = 10$ m x 100 m = 1000 m² = 0.001 km²

Based on an initial sample flight time of 1000 flight hours/year **total for all UAVs** which can cause injury to people, we get:

Number of flight hours over 50 years - fh50 = 50,000 (1,000 flight hours/year)

$p_{c/f}$ can now be calculated, = 1/(0.001 x 1 x 50,000) = 1/50

/Page 8/

Under the above conditions, including a total average number of flight hours of 1,000 per year for all UAV activity, it is thus possible to permit an accident frequency of 1 per 50 flight hours. In the long term this is naturally a too high probability to the power of ten, while on the other hand a crash frequency somewhat lower than for private planes should be permissible.

It then remains for the applicants to prove that it is likely that $p_{c/f}$ will not be more than 0.02 per flight hour.

With a higher number of flight hours, the requirements must be more stringent. For a total number of flight hours per year of 10,000 (100,000) in total for all UAV activity, the accident frequency must not be more than 1 per 500 (5,000) flight hours, with the other conditions mentioned above remaining constant. Other conditions produce other $p_{c/f}$s.

Finally, the individual risks over 80 years should be calculated for the persons living in areas above which UAVs are operated, with the total number of flight hours as intended over the foreseeable period extrapolated to a period of 80 years. The risk is independent of population density and is dependent amongst other things on the extent of the area within which operations take place, which can be shown by the following association:

ind. risk = $p_{c/f}$ x A_{lethal} x fh80/area < 1/25000 (based on all UAV operators together)

The larger the extent of the area, the smaller the individual risk for the same amount of UAV traffic. In an area of 100,000 km² there will be 50,000 people, if 0.5 people per km² live there on average. With a permitted (1) one death over a 50-year period, the individual risk will be (80/50)* 1/50000 = 0.000032 over an 80-year period, which is acceptable in comparison with a requirement of one per 25,000, or 0.00004. If on the other hand the area had been 1,000 km² with the same population density and the other conditions were the same, the individual risk of dying due to a crashing UAV would be 0.0032 over an 80-year period, which is 80 times too high a probability and would not be acceptable. This gives an indication that $p_{c/f}$ and/or A_{lethal} must be reduced or that the test/operating area must be increased.

3.3 Preliminary hazard analysis as regards risk of accidents

Based on a possible UAV system and the manner planned to operate it, the applicant should carry out a preliminary hazard analysis. This will start by listing (all) possible failure conditions at system level which could influence the UAV's ability to continue to operate safely. Such failure conditions would be expected to lead to an accident or a controlled interruption leading to an accident, which means a conservative assessment. The applicant should carry out this analysis at an early stage and also, where feasible, eliminate or reduce the effects of such failure conditions.

Internationally, such analyses are referred to as "preliminary hazard analyses".

Examples of such failure conditions are:

- Structural fracture, leading to probable accident
- A failure condition in the operating unit or UAV leading to loss or degrading (including erroneous data) of contact between the UAV and the operator

/Page 9/

- A failure condition in the operating unit or UAV leading to loss or degrading of contact with air traffic control (when such contact is required)
- Link disturbance, due to geometry, atmospheric turbulence, known fixed transmitters, other UAV systems, etc
- A failure condition in the UAV leading to difficulty in controlling the aircraft (or reduced ability to fly autonomously)
- A failure condition in the UAV making it more difficult to detect visually
- A failure condition in the UAV leading to degrading of the ability to see other aircraft (if such a system is installed)
- A failure condition in the UAV which means that the safety system is either not functioning or is functioning with restrictions
- An erroneous decision by the operator or air traffic controller due to erroneous, insufficient or misleading data.

The safety system and emergency procedures may be taken into account providing that their faults and limitations are also included in the conditions.

Hardware and software errors should be listed and analysed.

One suitable starting point to get ideas about undesirable failure conditions is the document *Suggested Flight Approval Process for Unmanned Air Vehicles (UAVs)* published by AeroVations Associates

Failure conditions which cannot be eliminated or suitably modified should subsequently be dealt with in line with their probability of occurrence. In the event of high probability, redundancy should be applied to reduce the probability.

For UAV systems where the operator keeps the UAV craft under constant, close, visual observation, a preliminary analysis as adumbrated above may be sufficient. For UAVs operating outside visual range the analysis must be complemented by qualitative probability assessments or preferably quantitative probability calculations before final operating approval can be granted after completed flight testing, thus giving a numerical value to pc/f.

3.4 Conditions for sharing airspace with manned aircraft

In the same way as with risks to persons on the ground, it is possible to state permitted probabilities for collisions between UAVs and manned aircraft during flight. It should also be possible to produce calculations for such probabilities. Another mode of approach is to state the operating limits under which UAVs are allowed to share airspace with manned aircraft based on current experience. We will ignore collisions between UAVs. These do indeed increase the probability of injury to persons on the ground, but in less densely populated areas it should be possible to ignore this possibility, due to the very low assessed probability of a collision between UAVs times the probability of persons being present in the crash areas.

The operating conditions for sharing airspace with manned aircraft will vary naturally, depending on where and how the operations are taking place. Considerations should be taken for:

/Page 10/

- The type of airspace (restricted zone, control zone, uncontrolled airspace, etc)
- The type of traffic (it is reasonable to impose stricter requirements on UAV systems where UAV traffic is mixed with heavy passenger traffic than when it mingles with recreational aircraft, aerial work, military aircraft and such like, for which a higher accident frequency is normally tolerated)
- Possible communication between the UAV and other aircraft and also UAV and ATS
- Air traffic density and predictability
- The weather conditions (will other traffic be able to see the UAV?)
- The type and version of link(s) to control the UAV
- The UAV's visibility (will other traffic be able to see the UAV?)

- The UAV's equipment (e.g. transponder, warning lights)
- The UAV's ability to see other traffic (autonomously or with the help of the operator)
- Any use of escort planes
- The operators' (mainly the "pilot's") training and experience
- Any specially allocated air traffic controller

The applicant should propose operating limits based on a qualitative analysis of the operational situation which will apply to all flights for which a permit is being sought. The Authority will then make an assessment and set the conditions.

4. ORGANISATION AND APPLICABLE SWEDISH CIVIL AVIATION REQUIREMENTS (BCL)

Each UAV system must be operated by an organisation who can demonstrate parity with the UAV system's complexity and operating conditions. For a smaller UAV system where the operator maintains close, visual contact, a relatively simple organisation will normally suffice.

The organisation should be of the same quality as corresponding organisations for the design of the relevant aviation with manned aircraft.

The organisation will probably vary at different stages of a project. During the design stage the emphasis may for example be on technical competence with advisory operational competence, while in the test stage further practical operational competence will be added and in the operational stage the emphasis will be on practical operating competence.

The organisation should ensure that the safety objectives set out in Section 2 will most likely be met (development phase) and be genuinely achieved during testing and operation.

/Page 11/

During the test stage, it may be necessary to impose special restrictions which can be removed later in the run-up to final operational approval.

To ensure that the safety objectives are met, the following guidelines will apply:

Key staff with sufficient competence should be appointed to be responsible for management, design, scrutiny, testing and normal running, depending on the stage, and to be responsible to the Aviation Safety Authority.

Preliminary and final hazard analyses must be approved by a competent scrutineer who is as far as possible organisationally separated from those responsible for construction. The preliminary analysis must be approved by the Authority before testing is permitted and the final analysis must be approved by the Authority before permanent approval can be granted.

The organisation must further ensure that BCLs are followed, which involves amongst other things:

- project approval being obtained from the Aviation Safety Authority at a relatively early stage after application
- design and manufacturing (for a new development) following the guidelines agreed with the Authority
- a written test programme with preliminary operating and emergency procedures being prepared
- a permit for test flying being obtained from the Authority, after application
- the test programme being followed or modified accordingly as lessons are learnt from the test
- written normal operating procedures being prepared and followed
- written emergency procedures being prepared and internalised
- a MEL (minimum equipment list (corresponding)) being prepared so that in the event of a failure in the field it is possible to look up any compensatory measures required for the operation to be permitted, e.g. any restrictions that may need to be imposed
- operators (pilots and system operators) being trained in the requirements commensurate with the complexity of operations
- competent technical staff seeing to preparation and maintenance
- other necessary permits being obtained from the Aviation Safety Authority and the Authority being kept informed about the project, including serious safety problems, at least to the extent stipulated in BCL-D1.3

Further guidelines can be obtained from the document *Suggested Flight Approval Process for Unmanned Air Vehicles (UAVs)* published by AeroVations Associates.

Each applicant should consider which BCL and JAR-OPS paragraphs are applicable to his special application. In general, the following BCLs apply:

/Page 12/

Airworthiness:

BCL-M 1.2, 1.3	(the form of registration and marking to be agreed with the Aviation Safety Authority from case to case
BCL-M 1.6	(relevant parts)
BCL-M 3.1, 3.2	(relevant parts)
BCL-M 4.2	
BCL-M 4.3	(parts relevant to IFR flying)

Operation:
BCL-T (including traffic rules, airspace, equipment)
Applicable parts of BCL-D from Series 1, inc. BCL-D 1.3 and D 1.9 (alternatively JAR-OPS 1.035) JAR-OPS 1 (or JAR-OPS 2 when so decided) relevant parts (including requirements as to organisation, handbooks, responsible staff, planning and monitoring, certain equipment requirements, training of operational staff).

Licensing and training:

In general, theoretical qualification requirements will be imposed corresponding to those applying to similar manned activity, as set out in JAR-FCL 1. Similarly, medical fitness requirements will apply corresponding to those for air traffic controllers. Provisionally, with this background, agreement can be reached between the applicant and the Authority from case to case and the exact requirement scenario will be established when deciding to grant an approval.

5.1 APPLYING FOR A PERMIT

Before any civil UAV may fly, an approval must always be obtained from the Aviation Safety Authority, also for flying within a restricted area. A military UAV may not be tested or operated in areas where civil aviation is permitted without a preceding consultation between FLYGI and the Aviation Safety Authority.

For a UAV system which is intended to be test-flown in stages outside a restricted area, it may be appropriate to inform the Authority in good time and give it an opportunity to study any experience gained. When participation from the Authority is desired or required, the rates set out in AIC Series B, latest version, will apply.

For a smaller UAV system where the operator maintains close visual contact, a permit application procedure can be applied which is simpler than as stipulated below.

In principle, two main routes are possible. One applies to systems which have been mainly developed and tested abroad, and which are to be tried for the first time in Swedish airspace. The second applies to Swedish UAV systems developed from scratch, or foreign systems which have not previously been tested, but which are to be tested in Swedish airspace.

An application should be submitted to the Aviation Safety Authority in both cases pursuant to BCL-M1.6 Section 4.1.

/Page 13/

In the first case, an application for a test flight permit pursuant to BCL-M1.6 Section 4.2.3 can be submitted at the same time, providing that the UAV system has been relatively well tested in some other country previously. Details and documents which appear applicable should be appended to this application pursuant to BCL M1.6 Sections 4.1 and 4.2. It is essential that the whole system is described clearly and that it demonstrates how the system is to be operated. A preliminary risk analysis should be appended to the application pursuant to Section 3.3 and a report on experience garnered from earlier flights, including statistics for accidents, faults and flight hours. The document *Suggested Flight Approval Process for Unmanned Air Vehicles (UAVs)* published by AeroVations Associates should as far as possible be followed. The Aviation Safety Authority may then request additional details and analyses. Specific requirements may need to be imposed on links (TBDs).

The organisation shall be described, and the operators' training status shall be mentioned.

If a Swedish UAV system is developed from scratch, an application for project approval should be sent to the Aviation Safety Authority pursuant to BCL-M1.6, Section 4.1. It is essential that the whole system be described clearly and that it is made clear how the system will be operated. This BCL should then be followed until approval of the system can be granted. However, references to design provisions are not fully applicable. A special agreement is required here with the Authority. Relevant parts of JAR-VLA, JAR-22, JAR-23, JAR-25, JAR-27 or

JAR-29 may be applicable to the aircraft itself, however. Further specific requirements may have to be imposed for the links. An application for a flight testing permit should be made pursuant to BCL-M1.6, Section 4.2.3. A preliminary risk analysis should be appended to the application pursuant to Section 2.4. The document *Suggested Flight Approval Process for Unmanned Air Vehicles (UAVs*, published by AeroVations Associates, should be followed as far as possible.

For foreign systems which have not previously been tested, the same principles will apply as for Swedish UAV systems. To the extent that the required information cannot be supplied to the Authority, special operating limits may be necessary, or a flight testing permit may be refused, which also applies to the other cases of course.

A maximum permitted value for $p_{c/f}$ should be agreed with the Authority during the application procedure.

When the Authority considers that the requirements for a flight testing permit have been fulfilled, a permit will be issued stating the conditions and restrictions.

The Authority should be given an opportunity to witness the test flights to the extent that it considers necessary.

When the test flight has been concluded and the applicant (normally after various modifications, about which the Authority should be informed) desires permanent approval to operate the system, an application to this effect should be submitted to the Authority.

A report should be appended to the application concerning test flights carried out together with a comprehensive, final safety analysis, possibly including special analyses of various subsystems to substantiate these. The analysis should show that the system safety objectives set out in Section 2 will probably be fulfilled under the proposed operating conditions.

/Page 14/

An application for permanent approval to operate a UAV system should also include details of the organisation and operators who will run the system.

/Page 15/

6. VARIOUS VIEWPOINTS ON SAFETY ANALYSES AND COMPUTER SYSTEMS

The System Safety Analysis (SSA) shall also account for the applicable (control, operating and other) measures needed to reduce the probability and mitigate the effect of various failure conditions. These should also be shown in checklists, the flight manual and the maintenance manual.

It has normally proved to be the case that so-called common mode failures are wrongly treated as failures, arising independently of each other, which gives an underrating of probabilities and possibly also of the consequences. The value of in-built redundancies can be thereby considerably reduced. In analyses, special stress should thus be laid on detecting such common mode failures.

When using redundancy in computer systems, dissimilar hardware and software can be used to minimize such common mode failures.

Each analysis must state the intended interfaces.

In addition to pure failure occurrences, the analyses should also take into account significant data inaccuracies.

The final result of system analyses should, if possible, be set out in the form of a fault tree.

However, fault tree analyses are not suitable for all types of digital systems. For systems or part-systems where one or more computers is playing an essential role, so-called "criticality" must be determined for the system, i.e. how dependent flight safety is on system function. This "criticality" will determine the extent of the verification of the computer (system) software which will be required. For airborne equipment methods should be applied pursuant to the document *Software consideration in airborne systems and equipment certification*, RTCA DO-178B/EUROCAE ED-12B. This document should also be used for so-called critical software in UAV systems (irrespective of whether the critical software is airborne or part of a subsystem on the ground).

As regards computers and software of the (commercial) off-the-shelf variety, COTS, the means is often lacking for an acceptable method to verify the quality of the design, manufacture and programming. It must therefore be assumed that failure conditions can arise in these products which cannot be foreseen and which may lead to risks with such periodicity that they cannot fulfil the objectives set for flight safety.

Flight safety objectives mean that an applicant must show how the objective can be achieved or maintained also in the event of hardware or software errors in off-the-shelf products if these are intended for use in subsystems critical for flight safety. For example, alarm functions will be needed to make the operator immediately aware that a fault has occurred. In addition, operational methods that can compensate in the event of failure and maintain acceptable flight safety need to be described.

If this is not possible and normal quality verification cannot be demonstrated, off-the-shelf products should not be used in subsystems critical to flight safety.