RPAS Integration in Switzerland
A holistic Approach

ICAO RPAS Symposium, 24. March 2015
Workshop 1, Airworthiness
Our starting point

- We need to ensure a safe aviation system.
- RPAS are “tools” to perform certain tasks.
- Commercial or not is not of importance.
- Operators need to fly to get experience with the RPAS and if there is a business case for them.
- We need to treat them proportional to the risk they pose to 3rd parties.
- We need to ensure equal treatment.
- We all have limited resources.
A balancing act...

Market growth

- Allow operations
- Gain experience

Safety

- Current aviation culture
- Current aviation rules
- Lack of harmonization
A balancing act...

- Market growth: Allow operations, Gain experience
- Safety: Rules proportionate to risk, GALLO
Resulting Concept in Switzerland

No additional risk mitigation

- (Below 30kg)
- Within direct visual contact (VLOS)
- Not within a distance of less than 100 meters around crowds (outdoors)
- > 5km Distance to civil & military airports/aerodromes
- < 150m AGL within a CTR
- Commercial ops allowed

Additional risk mitigation

- Operation inside the approved RPAS design envelope.
- Operation is part of the approved Operation Certificate scope.
- Operation is part of the approved crew qualification
- NOT POSSIBLE IN SWITZERLAND TILL 2016

No additional risk mitigation

- Authorisation Certification)
Specifics of the «?» ops category

- Wide variety of operations, very difficult to categorize
- Wide range of expertise among applicants
  - Small start-ups (no money, no time, great people, great ideas)
  - Photographers with NO aviation experience
  - Meteorologists with NO aviation experience
  - Military

- Wide range of RPAS
  - COTS (e.g. Phantom S-800)
  - Amateur built
  - Custom built for specific operation

- Huge economic potential if allowed to grow
- But «normal» Airworthiness Certification will not help!
A change in strategy – out of comfort zone!

[Blackboard drawing with the text:

- Where the magic happens
- RPAS
- Your Comfort Zone]
A change in culture, from atomistic...
Back to basics - Safety of RPAS
Total Hazard and Risk Assessment

- A tool to determine, if the risks are acceptable and what safety barriers/mitigations need to be established.
- These safety barriers can affect the RPAS and the operational environment.
- **Therefore, detailed information are required about:**
  - Operator
  - Operation
  - RPAS incl. Datalink & QMS (configuration control, change management, CAW, etc.)
  - Proposed Limitations

- The advantage of a Total Hazard and Risk Assessment as above is, that it can be used as well, to determine the applicable certification basis for a product (CS-LURS/LUAS.1).
Guidance for an Authorisation for Low Level Operation of RPAS

- A Total Hazard and Risk Assessment as required e.g. in CS-LURS
- Technical shortcomings can be mitigated by operational limitations[…]
- Allows operations where normal airworthiness certification is impractical

1. What happens if [...]?
2. Why this can happen?
Event Sequence Diagram
A practical example

1500 m AGL
What happens if [...]?

Loss of Control

Fly Away

20 m

200 m

1500 m

RPAS Integration in Switzerland • A holistic Approach
Markus Farner, Swiss FOCA
What happens if [...]?

- Loss of Position Data
- Loss of Propulsion
- Loss of Electrical Energy
- Loss of C2 Link
- External Conditions
- Crew Error

- Fly Away
  - Separation Conflict
    - MAC
  - GND Impact
    - ERC
    - Hazard to people
    - Hazard to Infrastructure
What happens if [...]?

1. Loss of Control
   - Loss of visual Contact
     - Crew failed to activate ERC
       - ERC failed to activate
         - Flight abort
       - ERC failed to activate
         - Fly Away
     - Crew failed to activate ERC
       - Fly Away
   - Loss of Position Data
     - Fly Away

YES

NO
## Safety barriers “log”

<table>
<thead>
<tr>
<th>Safety barrier</th>
<th>Related limitation/condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain visual contact with RPA at all times</td>
<td>1. Ops to be conducted at night (due to other safety barrier)</td>
</tr>
<tr>
<td></td>
<td>2. A light must be installed on the RPA and visible to ground crew at all times</td>
</tr>
<tr>
<td></td>
<td>3. No flight into clouds or when visibility does not allow visual contact with the RPA</td>
</tr>
<tr>
<td></td>
<td>4. «Return-to-home» to be initiated in case of failure of the light</td>
</tr>
<tr>
<td>Maintain Position Data</td>
<td>1. Second Position Data Source (GLONASS, INU, etc.)</td>
</tr>
<tr>
<td></td>
<td>2. Independent power supply</td>
</tr>
<tr>
<td></td>
<td>3. Etc...</td>
</tr>
<tr>
<td>...</td>
<td>1. ...</td>
</tr>
</tbody>
</table>
What happens if [...]?

- Loss of Control
  - Loss of visual Contact
    - Loss of Position Data
      - Fly Away
  - Crew failed to activate ERC
    - ERC failed to activate
    - Fly Away
    - Flight abort
  - YES
- NO
## Safety barriers “log”

<table>
<thead>
<tr>
<th>Safety barrier</th>
<th>Related limitation/condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure flight crew awareness, to initiate the ERS when required</td>
<td>1. Crew training</td>
</tr>
<tr>
<td></td>
<td>2. Additional observer</td>
</tr>
<tr>
<td></td>
<td>3. Etc...</td>
</tr>
<tr>
<td>Adequate ERS maintenance</td>
<td>1. ERS maintenance in Authorisation</td>
</tr>
<tr>
<td></td>
<td>2. ERS operation cycle log</td>
</tr>
<tr>
<td></td>
<td>3. Etc...</td>
</tr>
<tr>
<td>…</td>
<td>1. …</td>
</tr>
</tbody>
</table>

*RPAS Integration in Switzerland • A holistic Approach*

Markus Farner, Swiss FOCA
What happens if [...]?

- Loss of Position Data
- Loss of Propulsion
- Loss of Control Energy
- Loss of C2 Link
- External Conditions
- Crew Error

Loss of Control → Fly Away

- Separation Conflict
  - MAC
  - ERC

Fly Away →

- GND Impact
  - Hazard to people
  - Hazard to infrastructure

RPAS Integration in Switzerland • A holistic Approach
Markus Farner, Swiss FOCA
What happens if [...]?

Separation Conflict

Automatic Separation failed

ATC failed to detect conflict

AC Pilot failed to detect conflict

Conflict AC failed to avoid

MAC

MAC

Separation

YES

NO
Why this can happen [...]?

Loss of Position Data

Loss of Propulsion

Loss of Energy

Loss of C2 Link

External Conditions

Crew Error

Loss of Control

Fly Away

MAC

Separation Conflict

ERC

Hazard to people

GND Impact

Hazard to Infrastructure
Why this can happen [...]?

- Loss of Propulsion
  - Inadequate Maintenance
    - Inadequate Maintenance Crew
    - Inadequate Maintenance Data
  - Energy leakage
    - Technical problem
  - Human problem
  - Inadequate Operation planning
    - Inadequate OPS Planning Crew
    - Unsufficient Planning Data

- Inadequate Maintenance
- Energy leakage
- Inadequate Operation planning
SAFETY BARRIER: Maintain visual contact with RPA

Bow Tie – why this can happen [...]?
## Safety barriers “log”

<table>
<thead>
<tr>
<th>Safety barrier</th>
<th>Related limitation/condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure all Data required to perform the intended operation is available</td>
<td>1. Respective Processes in place to transform the intended operation in adequate mission planning</td>
</tr>
<tr>
<td></td>
<td>2. Training of involved personnel</td>
</tr>
<tr>
<td></td>
<td>3. Etc...</td>
</tr>
<tr>
<td>Ensure, energy leakage will not result in a loss of control</td>
<td>1. No single energy source</td>
</tr>
<tr>
<td></td>
<td>2. Ground Crew training</td>
</tr>
<tr>
<td></td>
<td>3. Pilots training</td>
</tr>
<tr>
<td></td>
<td>4. Etc...</td>
</tr>
<tr>
<td>...</td>
<td>1. ...</td>
</tr>
</tbody>
</table>
Resulting 3 Safety Modules

Holistic Approach

Total Hazard and Risk Assessment

Implement the Safety Barriers out of the Assessment

Safe RPAS Operation
### Safety barriers “log” extend it further

<table>
<thead>
<tr>
<th>Safety barrier</th>
<th>Related limitation/condition</th>
</tr>
</thead>
</table>
| Ensure safe separation to other aircrafts in uncontrolled airspace | 1. Fly where no VFR traffic is flying (close to obstacles, direct in clouds...)  
2. Stay away from any IFR routes (coordinate with ANSP)  
3. Etc...                                                                 |
| Ensure operational safety in icing conditions      | 1. Procedures to abort the flight in case icing accumulation affects the performance (power)  
2. No people NOT under operator control in the operation area  
3. Anti Icing on ERS  
4. Etc...                                                                 |
| ...                                                | 1. ...                                                                                      |
Risk model and accident scenarios

- GALLO model based on results of ASCOS WP3.2 results
- 6 accident scenarios represented as ESD types (Event Sequence Diagram)
- Events are further detailed in Fault Trees

ESD type 1 – System failure
ESD type 2 – Datalink deterioration
ESD type 3 – Operations outside approved envelope/limitations
EDS type 4 – Fire
ESD type 5 – Loss of safe separation
ESD type 6 – Remote crew error
Conclusions

Guidance for an Authorization for Low Level Operation of RPAS

Provides a framework for the applicant to:

1. Collect information about his intended operation
2. Perform a structured technical review of the RPAS with focus on safety features related to the operation
3. Analyse the accident scenarios and identify the relevant safety barriers
4. Provide all this information to the authority in a standardized format
Conclusions

Guidance for an Authorization for Low Level Operation of RPAS

Provides a framework for the certifying authority to:

1. Build a comprehensive picture of the operation under approval
2. Understand the risks involved in the operation
3. Understand what safety barriers are in place to ensure safety of the operation
4. Invest the limited available resources on the verification of those barriers
Questions...
...and Answers...