Safety & Cyber-Security Analysis based on Systems-Theory
Carmen Frischknecht-Gruber, Christoph W. Senn, Sven S. Krauss, Monika U. Reif
ZHAW Zurich University of Applied Sciences, Switzerland
Agenda

1. Motivation
2. Related Work
3. Research Objectives
4. Case study: U-space
5. Conclusion and Outlook
Evolving Technology

2005

http://www.spiegel.de/panorama/bild-889031-473242.html

2013
Why Safety and Security Analysis?

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

https://www.telemedicineclinic.com/blog/wannacry-ransomware-hits-nhs-fails-interrupt-tmc-service/
The Need of a Safe and Secure U-space

The Need of a Safe and Secure U-space

Related Work
Related Work

Few studies available regarding safety, security and privacy of drones

- Schmittner C., Ma Z., Puschner P., 2016
- Plioutsias, A., Karanikas, N. and Chatzimihailidou, 2017
- ...

Limitations

- Focus is on reliability, safety and security of the drone as a system itself
- Integration into unmanned air traffic management system not considered yet

doi: 10.1109/ICTIS.2015.7232133

doi: 10.1007/978-3-319-45480-1_16

doi: 10.1111/risa.12867
Research Objective
Research Objective

Research Questions

- Safety and security analysis of the complete socio-technical system
- Consequences for UAS requirements and design

Hypothesis

- Potential conflicts safety vs. security

Research Method

- Case Study with public available material
- Perform STPA analysis
- Perform STPA-Sec analysis
- Summarizing the results

https://auterion.com/product/
U-space

Case Study
U-space Overview

Stakeholders

- EASA – European Aviation Safety Agency
- SESAR – Single European Sky ATM Research
- BAZL – Bundesamt für zivile Luftfahrt *
- Skyguide

* FOCA – Federal Office for Civil Aviation

SESAR, “U-space Blueprint”, SESAR Joint Undertaking, 2017
U-space Overview

Mission

- Ensure safety of all airspace users in operation
- Provide a scalable, flexible and adaptable system
- Manage the interface with manned aviation
- Enable high-density operations with multiple automated drones
- Follow a risk-based and performance-driven approach
- Set up appropriate requirements for safety, security

SESAR, "U-space Blueprint", SESAR Joint Undertaking, 2017
U-space Overview

Roadmap

- **Milestone 1 – 2019**
  - primarily online registration and identification as well as geofencing

- **Milestone 2 – 2021**
  - implement flight planning and airspace approval, live tracking and dynamic situational awareness

---

SESAR, “U-spaceBlueprint”, SESAR Joint Undertaking, 2017
U-space Overview

Roadmap

- Milestone 3 – 2023
  - more complex operations are possible and also more automation is available
  - increase of flights outside the visual range

- Milestone 4 – 2025
  - Fully automated, networked and digital infrastructure throughout the European Aviation Area

U-space Overview - Switzerland

Swiss U-space demonstrator run-through by skyguide
https://www.skyguide.ch/de/events-medien/u-space-live-demonstration/
Analysis

& Results
STPA and STPA-Sec Analysis

UAS Operation Management

Air Traffic Control

UAS Management System

Airspace Information

License Check

Flight Ban Map

Obstacle Map

Weather Info

Telemetry Data

Real Time Map

UAS Positions

MAS Positions

UAS Operator

UAS
<table>
<thead>
<tr>
<th>Loss</th>
<th>Hazard</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collision with UAS</td>
<td>UAS operator is unresponsive</td>
<td>UAS shall have a self-supporting collision avoidance system</td>
</tr>
<tr>
<td>Loss of cargo</td>
<td>UAS opens cargo bay unintentionally</td>
<td>UAS cargo bay shall have a fail-safe locking mechanism</td>
</tr>
</tbody>
</table>
# Hazards, Losses, Safety Constraints

<table>
<thead>
<tr>
<th>Loss</th>
<th>Hazard</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collision with UAS</td>
<td>UAS operator is unresponsive</td>
<td>UAS shall have a self-supporting collision avoidance system</td>
</tr>
<tr>
<td>Loss of cargo</td>
<td>UAS opens cargo bay unintentionally</td>
<td>UAS cargo bay shall have a fail-safe locking mechanism</td>
</tr>
<tr>
<td>Loss of UAS</td>
<td>UAS is operated by unauthorized person</td>
<td>UAS shall only be flown by authorized person(s)</td>
</tr>
</tbody>
</table>
Example: Flight modification

1. Flight modification
   - Not provided when expected
   - UAS Operator does not initialize flight modification when requested
   - UAS does not free space in emergency situation
   - UAS shall have a safe self-supporting avoidance and landing system
   - Airspace shall be freed within time constraint
   - UAS does (intentionally) not free airspace when requested
   - UAS does not free space in emergency situation
   - UAS shall have a safe self-supporting avoidance and landing system
   - Airspace shall be freed within time constraint
   - UAS is operated by unauthorized person
   - An external emergency control system shall be provided (!)

- Collision with MAV
- Collision with UAS
- Intentionally hazardous flying behaviour
Example: Flight modification

STEP 2

UAS Operator

Real time position, UAS state

Sensor System UAS

- GPS
- Speed
- Altitude
- ...

UAS in Operation

Sensor readouts

Flight modification

UAS controller

Low-level control action

UAS Operator does not initialize flight modification when requested

UAS does (intentionally) not free airspace when requested
## Example: Flight modification

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Causal Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAS Operator does not initialize flight modification when requested</td>
<td>• Information flow between UAS and UTM is interrupted</td>
</tr>
<tr>
<td></td>
<td>• Information flow between UAS and UTM is corrupted</td>
</tr>
<tr>
<td>If external input is incorrect, then…</td>
<td></td>
</tr>
<tr>
<td>UAS does not adjust trajectory when UTM requested it</td>
<td></td>
</tr>
<tr>
<td>If the process model is incorrect, then…</td>
<td>• Command processing is erroneous</td>
</tr>
<tr>
<td></td>
<td>• UAS controller is maliciously modified</td>
</tr>
<tr>
<td>UAS adjusts trajectory incorrectly when UTM requested it</td>
<td></td>
</tr>
<tr>
<td>If CA is not given or erroneous, then…</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS does not adjust trajectory or is adjusting it incorrectly when UTM</td>
<td></td>
</tr>
<tr>
<td>requested it</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Causal Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Example: Flight modification

<table>
<thead>
<tr>
<th>UAS Operator does not initialize flight modification when requested</th>
<th>Scenario</th>
<th>Causal Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>If actuator is delayed or not acting at all, then…</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If process input is wrong at UAS, then…</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If feedback is given incorrectly or not at all to sensors, if sensors operate incorrectly, then…</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If feedback given too late, then…</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Preliminary Analysis Results

Preliminary findings

- Regulations in emergency situations must be clarified
- Emergency and intervention mechanism are needed
- Prioritisation concept for UAS
- Data must be reliable and tested for its accuracy during operation
- High security standards are needed → remote access to UAS?
- Unclear growth of U-space → Scaling?
Conclusion & Outlook
Conclusion and Outlook

Results

- STPA and STPA-Sec provide reasonable outcomes
- Conflicting measures can be found

Outlook

- Analysis must be conducted in more detail
- Security part might be overworked, since STPA-Sec does not provide a best practice – might need more assistance
- Same goes for STPA in general – applying lessons learned to the new analysis – Abstraction level
- Clarify uncertainties with experts
- Conduct expert interviews

«STPA and STPA-Sec do provide a good starting point for a full analysis. It could be seen as a basis or fundamental structure for more safety and security analysis techniques»
For further questions, I am now at your disposal.

Carmen Frischknecht-Gruber
frsh@zhaw.ch

Christoph Walter Senn
senh@zhaw.ch

Sven Stefan Krauss
krav@zhaw.ch

https://auterion.com/product/
Appendix
Personal details

To complete your registration, please fill in your details below.

First name *
Hal

Last name *
Smith

Date of birth *
1988-09-22

Company
AirMap

Mobile phone number *

Back
Next
Drone pilot ground control station
Obstacle map and flight zone map by BAZL/FOCA