Zurich University
of Applied Sciences

School of
Engineering
IAMP Institute of Applied
Mathematics and Physics

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

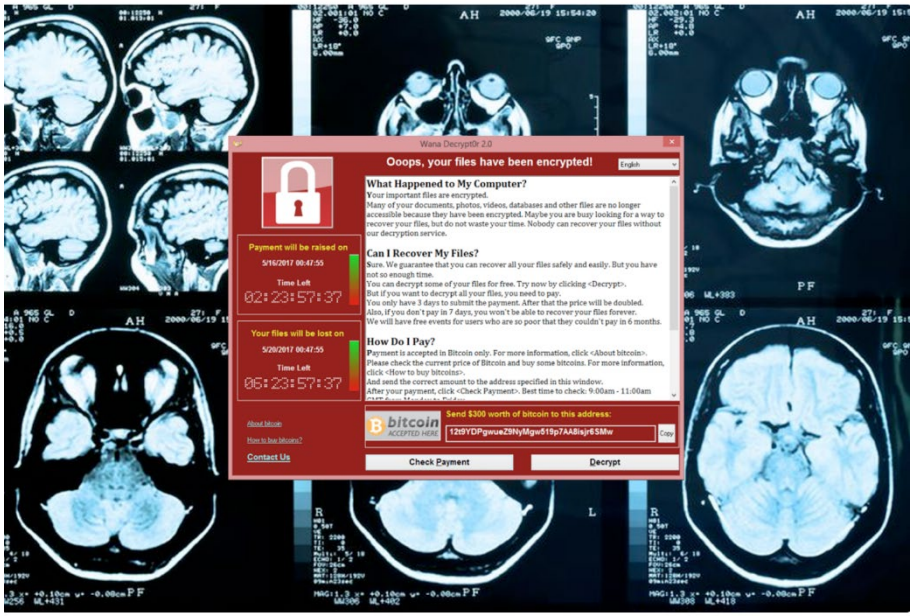
http://www.spiegel.de/panorama/bild-889031-473242.html

2005

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

https://www.ibtimes.co.uk/dark-side-drone-police-reveal-uavs-being-used-theft-smuggling-spying-children-1523662#slideshow/1463177

The Need of a Safe and Secure U-space

https://www.berliner-kurier.de/berlin/polizei-und-justiz/tourist-verletzt-kamera-drohne-stuerzt-auf-alex-22493330

Related Work

Related Work

Related Work

Few studies available regarding safety, security and privacy of drones

- J. Chen, S. Zhang, Y. Lu and P. Tang, 2015
- 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

J. Chen, S. Zhang, Y. Lu and P. Tang, (2015), "STPA-based hazard analysis of a complex UAV system in take-off," *2015 International Conference on Transportation Information and Safety (ICTIS)*, Wuhan, pp. 774-779.
doi: 10.1109/ICTIS.2015.7232133

Schmittner C., Ma Z., Puschner P. (2016), Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis. In: Skavhaug A., Guiochet J., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, vol 9923. Springer, Cham
doi: 10.1007/978-3-319-45480-1_16

Plioutsias, A. , Karanikas, N. and Chatzimihailidou, M. M. (2018), "Hazard Analysis and Safety Requirements for Small Drone Operations: To What Extent Do Popular Drones Embed Safety?. Risk Analysis, 38: 562-584.
doi:10.1111/risa.12867

Research Objective

Research Objective

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

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/

EASA European Aviation Safety Agency

JARUS
JOINT AUTHORITIES FOR RULEMAKING ON UNMANNED SYSTEMS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Office of Civil Aviation FOCA

skyguide

auterion

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-spaceBlueprint", SESAR Joint Undertaking, 2017
https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF

U-space Overview

Mission

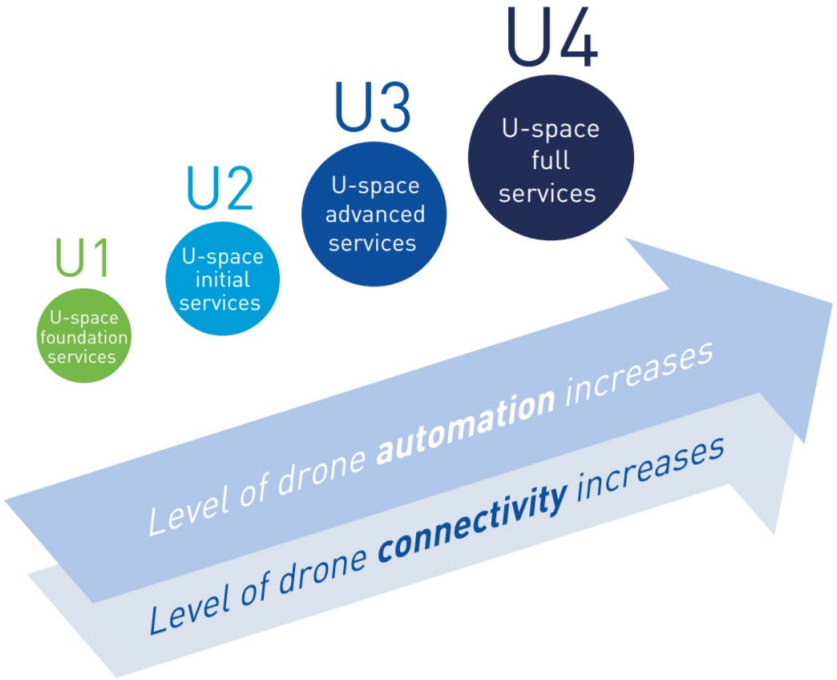
- Ensure safety of all airspace users in operation
- Provide a scalable, flexible and adaptable system
- Manage the interface with manned aviation
- Enable high-density operations with multiple automated drones
- Follow a risk-based and performance-driven approach
- Set up appropriate requirements for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

SESAR, “U-spaceBlueprint“, SESAR Joint Undertaking, 2017
https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF

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

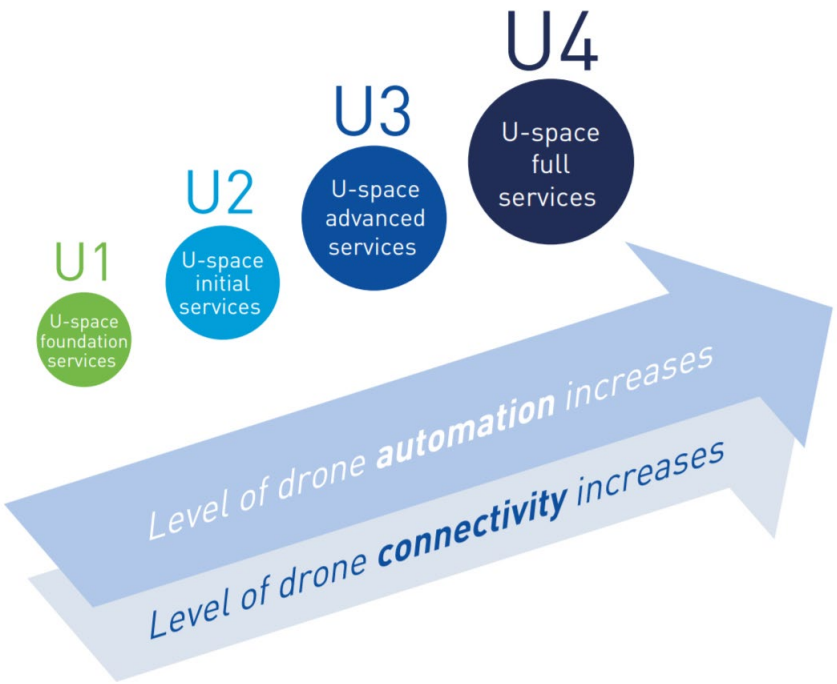


SESAR, "U-spaceBlueprint", SESAR Joint Undertaking, 2017
https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF

U-space Overview

Roadmap

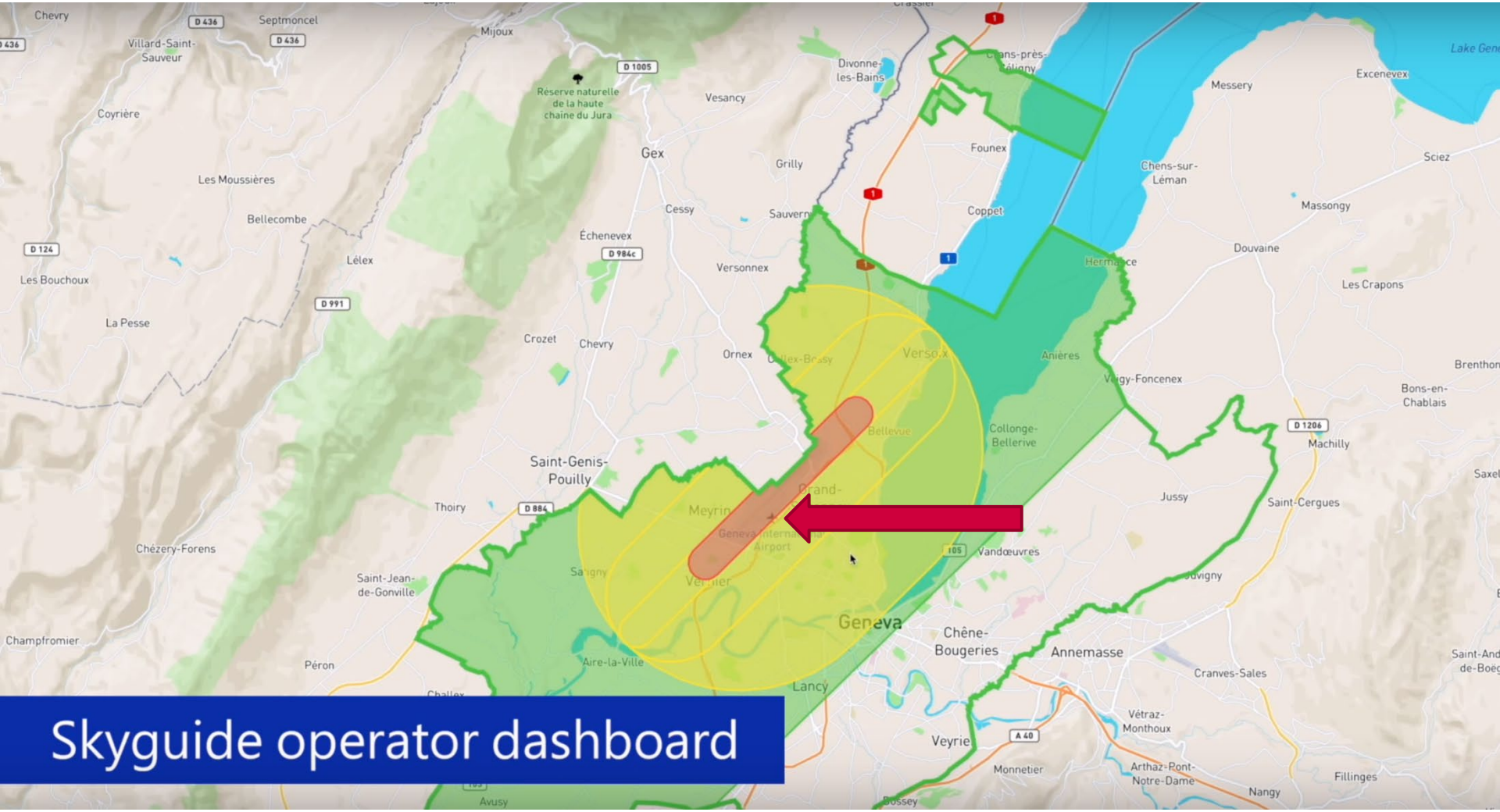
- Milestone 3 – 2023
  - more complex operations are possible and also more automation is available
  - increase of flights outside the visual range
- Milestone 4 – 2025
  - Fully automated, networked and digital infrastructure throughout the European Aviation Area



SESAR, "U-spaceBlueprint", SESAR Joint Undertaking, 2017
https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF

U-space Overview - Switzerland

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

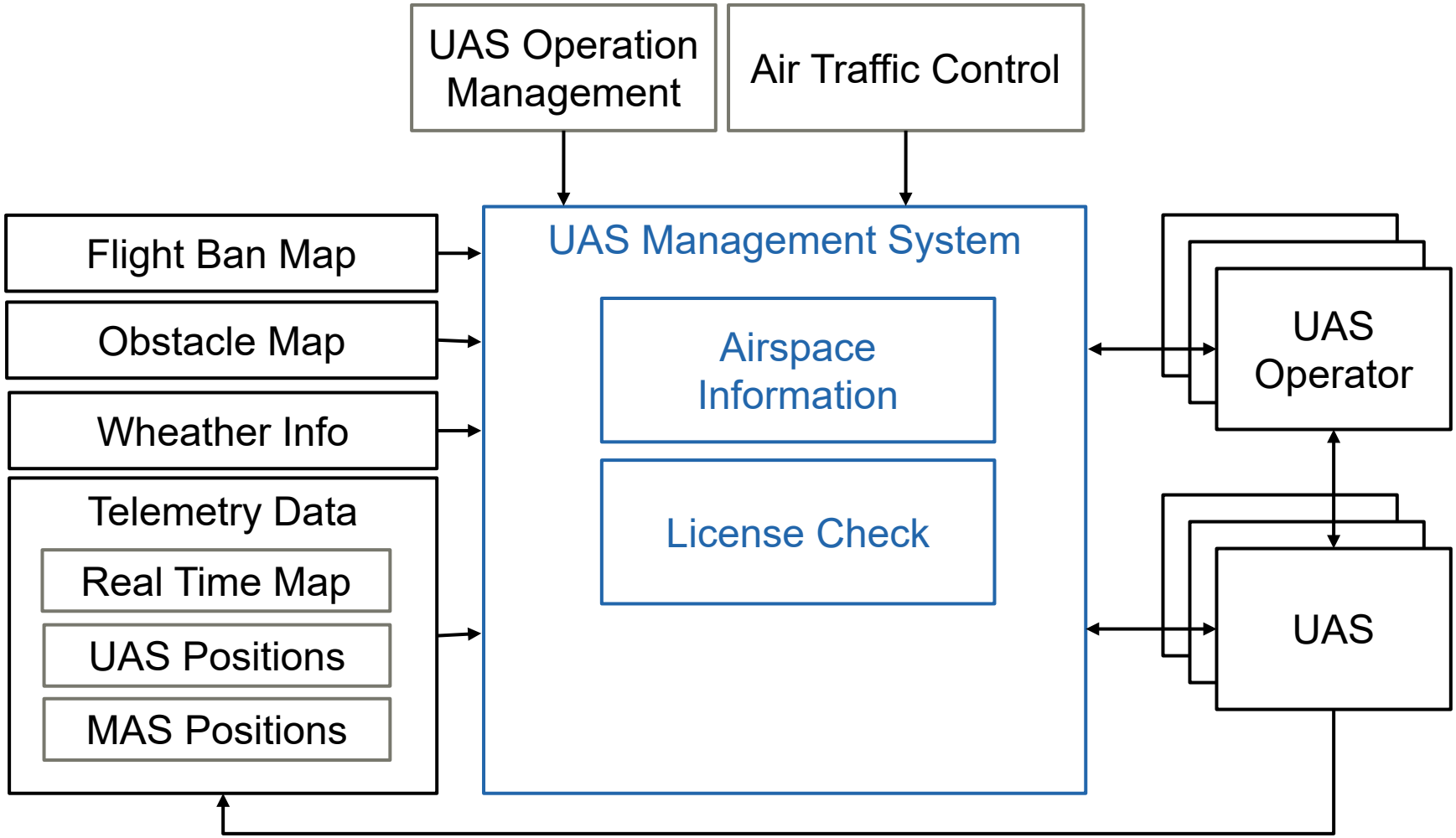


Swiss U-space demonstrator run-through by skyguide
https://www.skyguide.ch/de/events-medien/u-space-live-demonstration/

Analysis

& Results

STPA and STPA-Sec Analysis

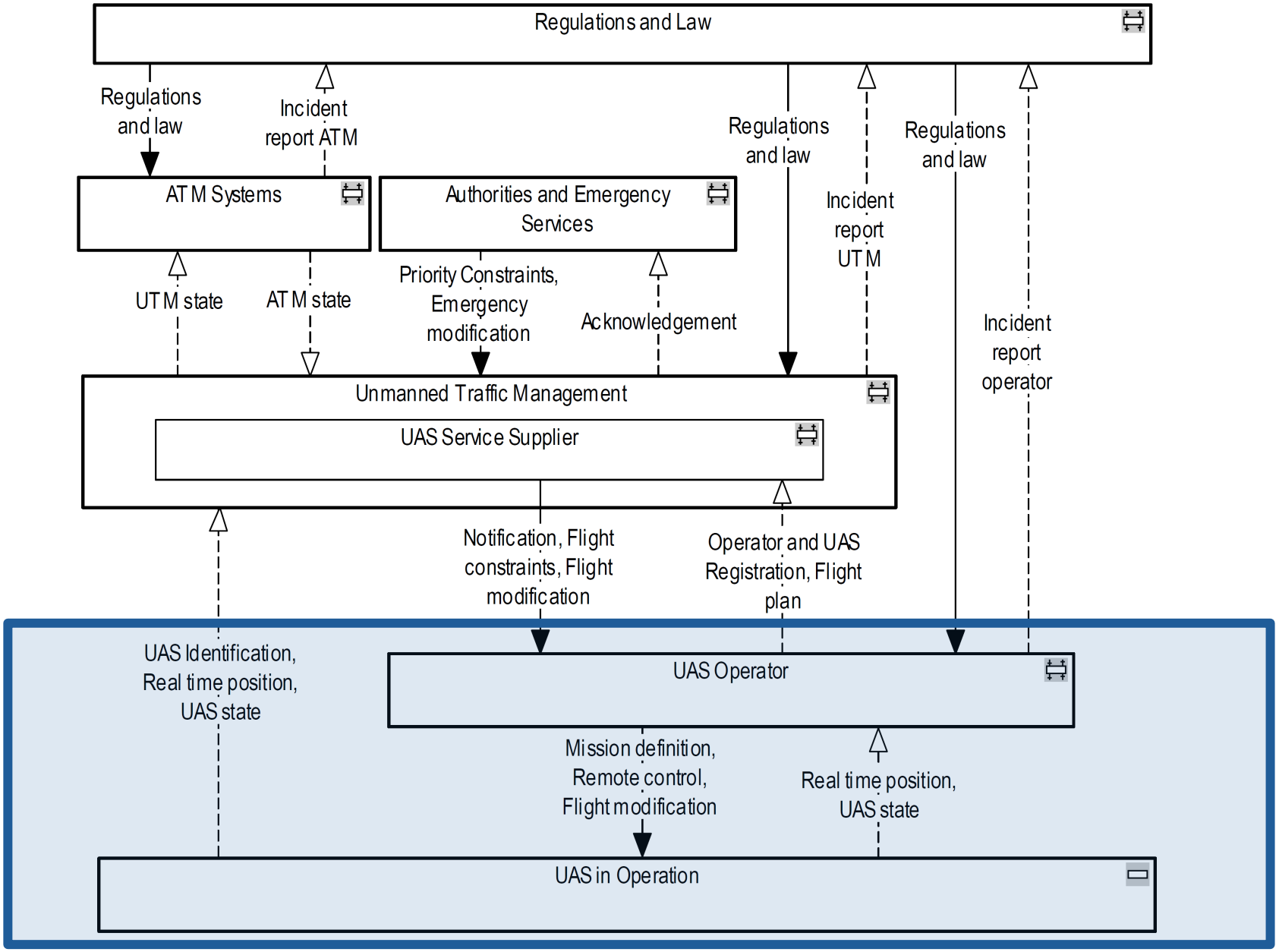


Hazards, Losses, Safety Constraints

Loss	Hazard	Safety Constraint
Collision with UAS	UAS operator is unresponsive	UAS shall have a self-supporting collision avoidance system
Loss of cargo	UAS opens cargo bay unintentionally	UAS cargo bay shall have a fail-safe locking mechanism

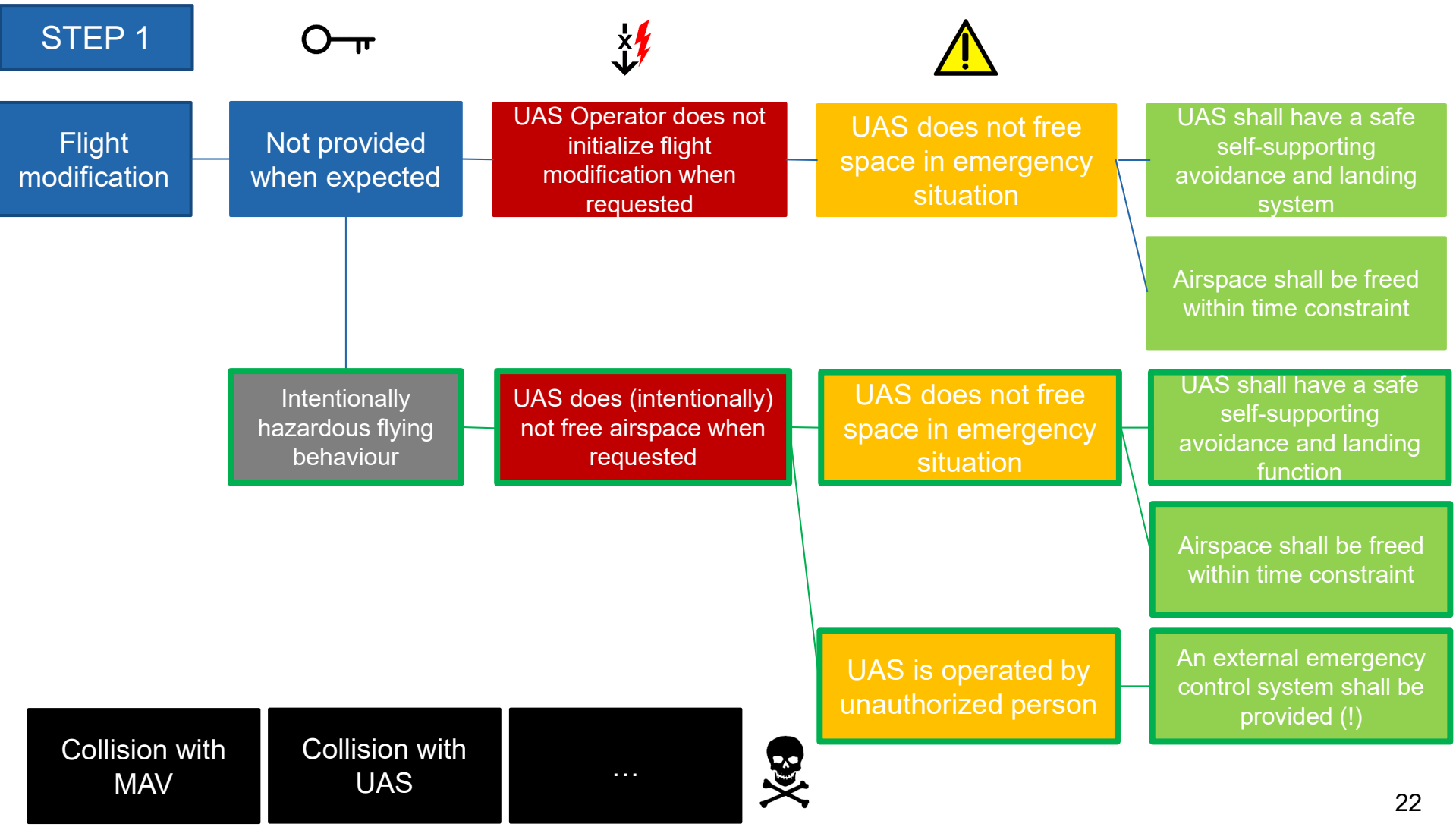
Hazards, Losses, Safety Constraints

Loss	Hazard	Safety Constraint
Collision with UAS	UAS operator is unresponsive	UAS shall have a self-supporting collision avoidance system
Loss of cargo	UAS opens cargo bay unintentionally	UAS cargo bay shall have a fail-safe locking mechanism
Loss of UAS	UAS is operated by unauthorized person	UAS shall only be flown by authorized person(s)


Regulations and Law
Regulations and law
Incident report ATM
Regulations and law
Regulations and law
ATM Systems
Authorities and Emergency Services
Incident report UTM
UTM state
ATM state
Priority Constraints, Emergency modification
Acknowledgement
Incident report operator
Unmanned Traffic Management
UAS Service Supplier
Notification, Flight constraints, Flight modification
Operator and UAS Registration, Flight plan
UAS Identification, Real time position, UAS state
UAS Operator
Mission definition, Remote control, Flight modification
Real time position, UAS state
UAS in Operation

Example: Flight modification

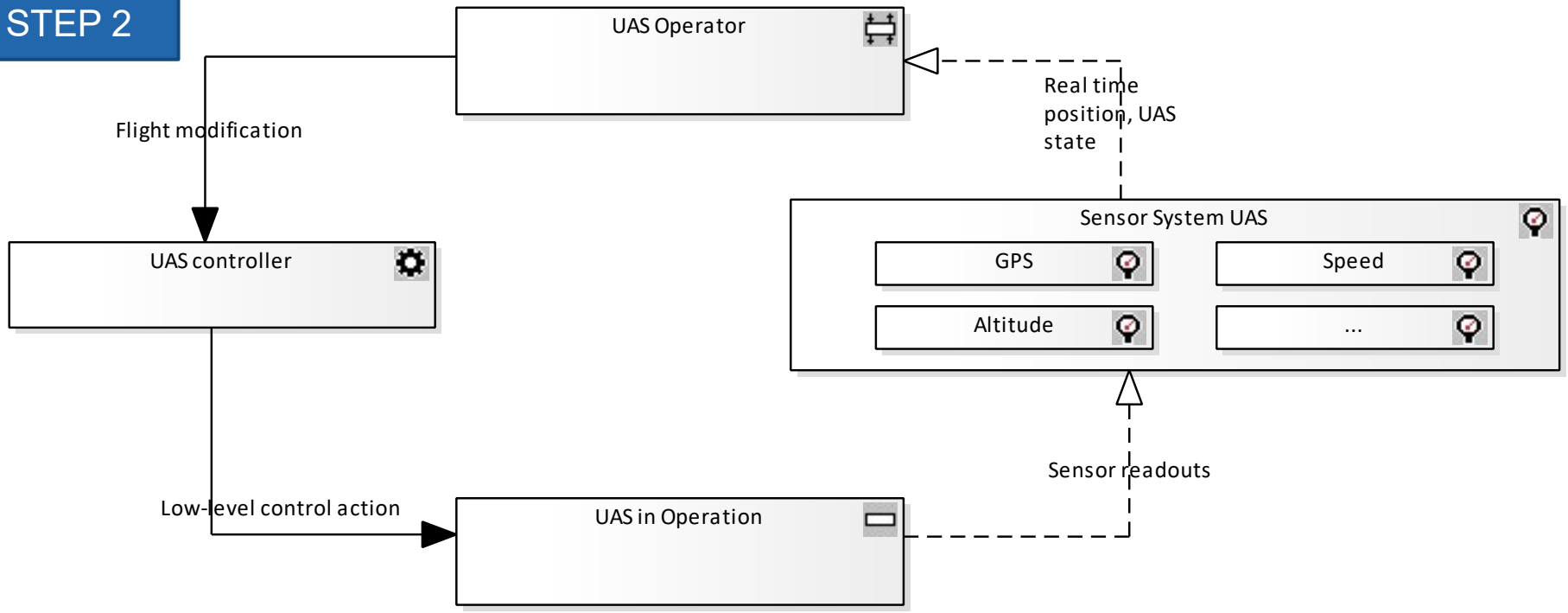
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



Example: Flight modification

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

STEP 2



UAS Operator does not initialize flight modification when requested

UAS does (intentionally) not free airspace when requested

Example: Flight modification

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

Example: Flight modification

UAS Operator does not initialize flight modification when requested	Scenario	Causal Factor
If actuator is delayed or not acting at all, then…		
If process input is wrong at UAS, then…		
If feedback is given incorrectly or not at all to sensors, if sensors operate incorrectly, then…		
If feedback given too late, then…		

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»

https://auterion.com/product/

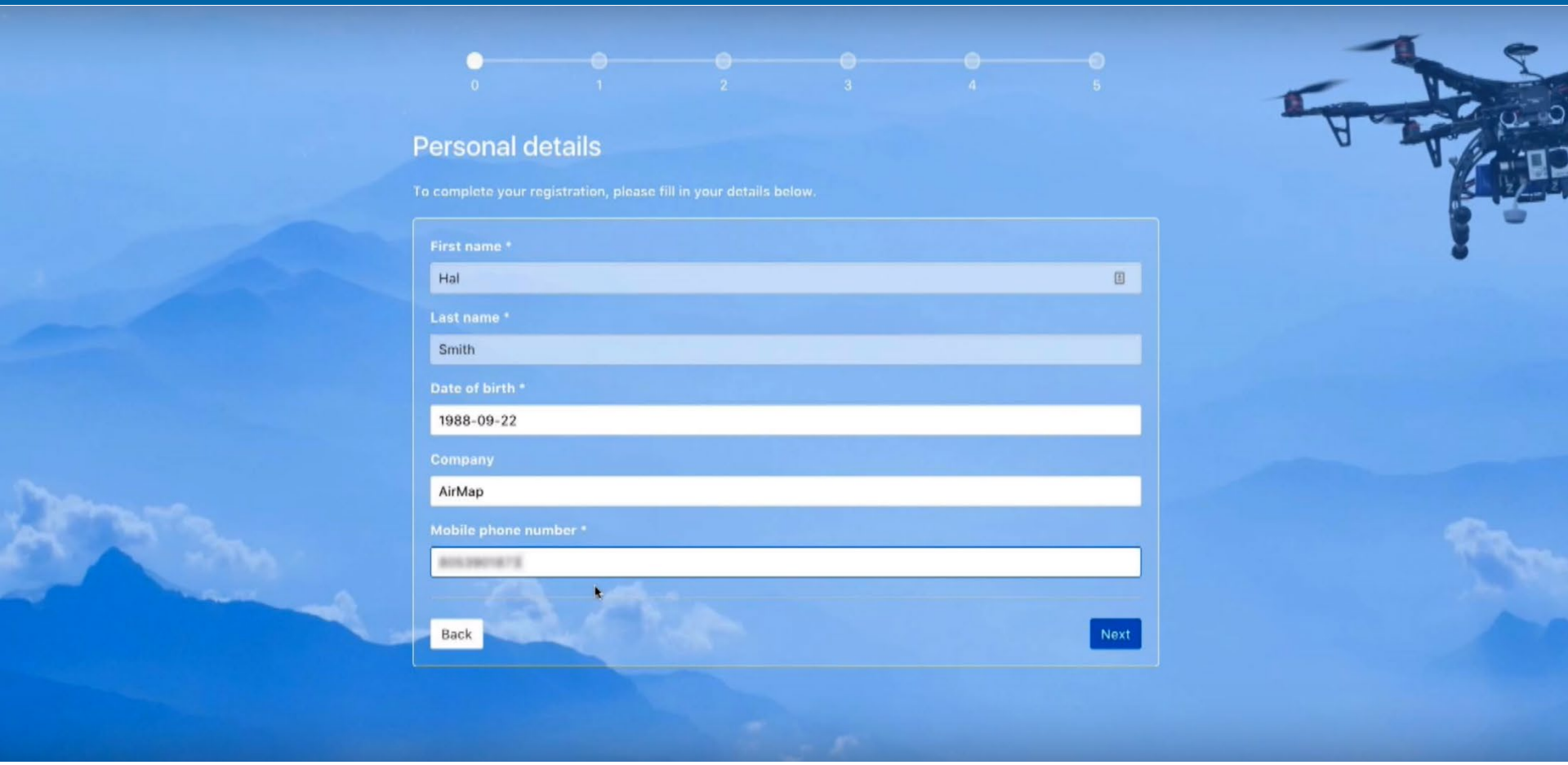
Carmen Frischknecht-Gruber
frsh@zhaw.ch

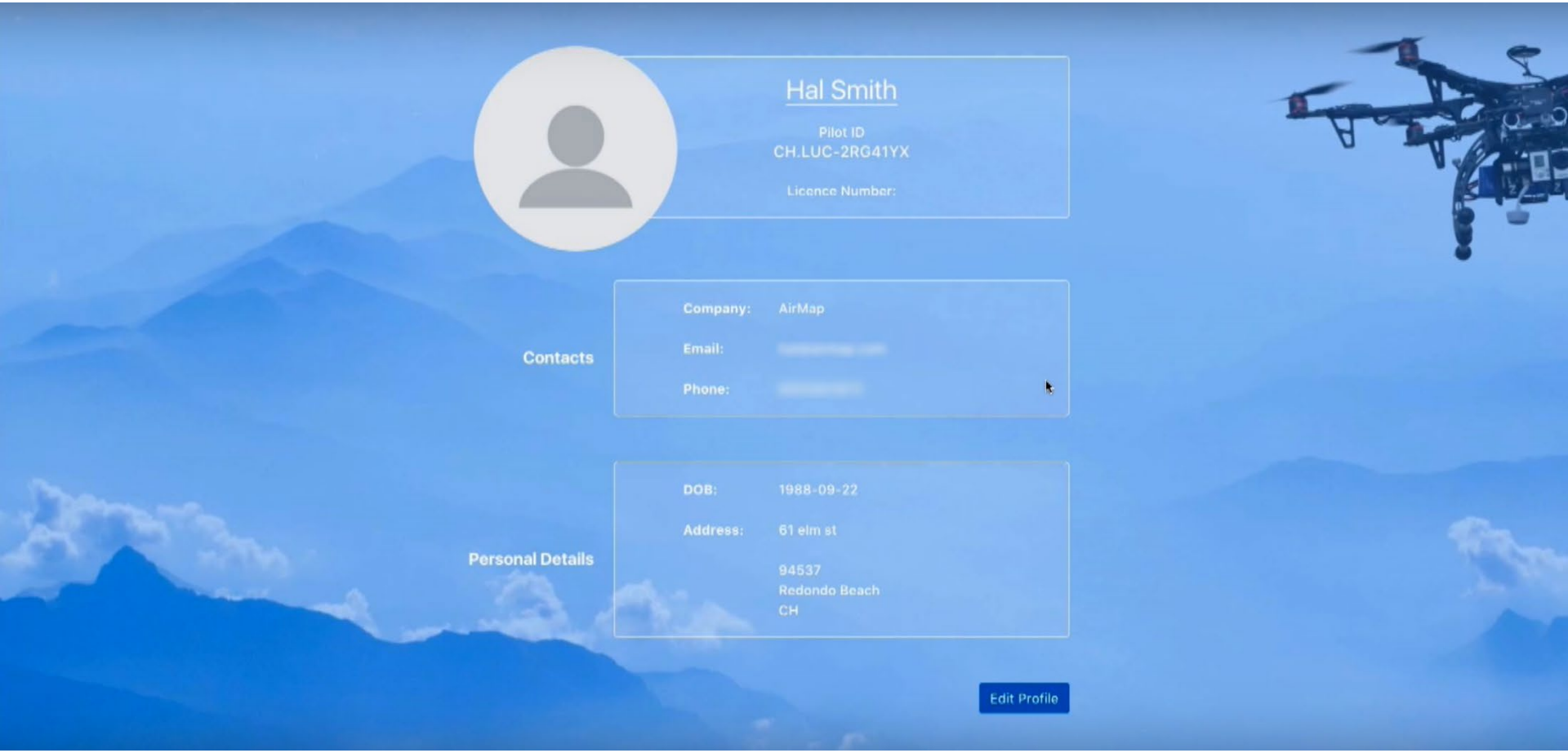
Christoph Walter Senn
senh@zhaw.ch

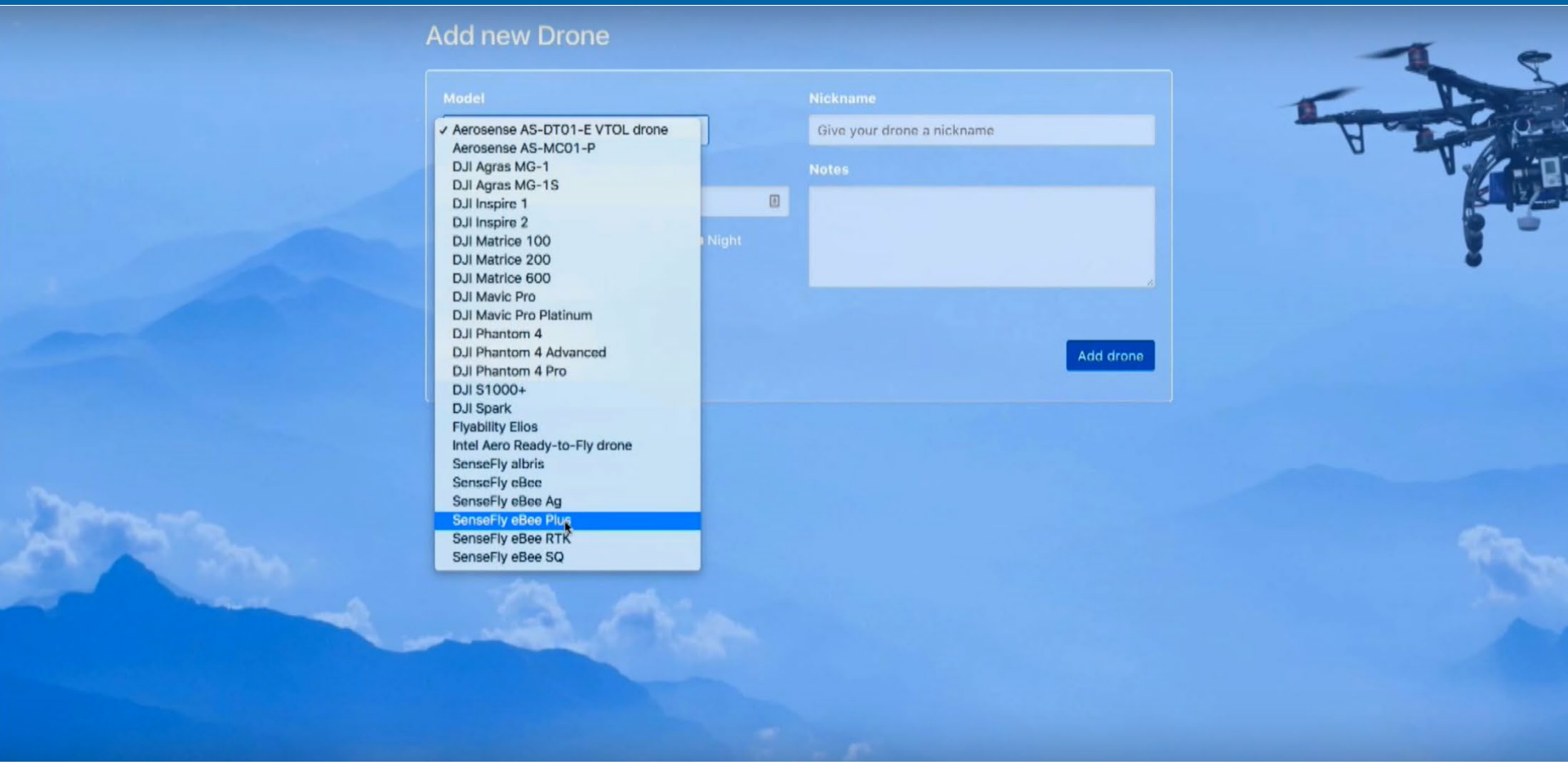
Sven Stefan Krauss
krav@zhaw.ch

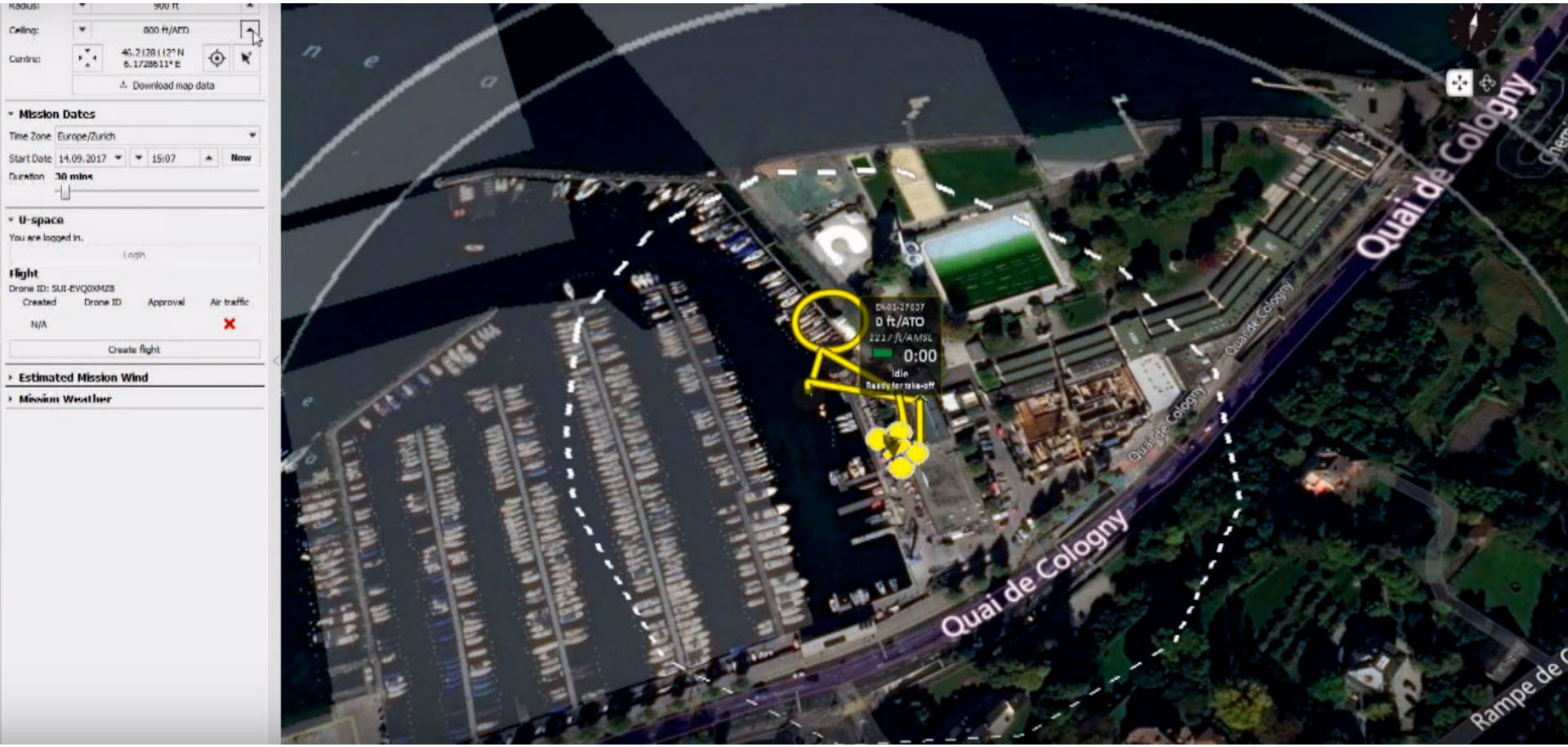
For further questions, I am now at your disposal.

Appendix


0
1
2
3
4
5
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


Hal Smith
Pilot ID
CH.LUC-2RG41YX
Licence Number:
Contacts
Company: AirMap
Email:
Phone:
Personal Details
DOB: 1988-09-22
Address: 61 elm st
94537
Redondo Beach
CH
Edit Profile

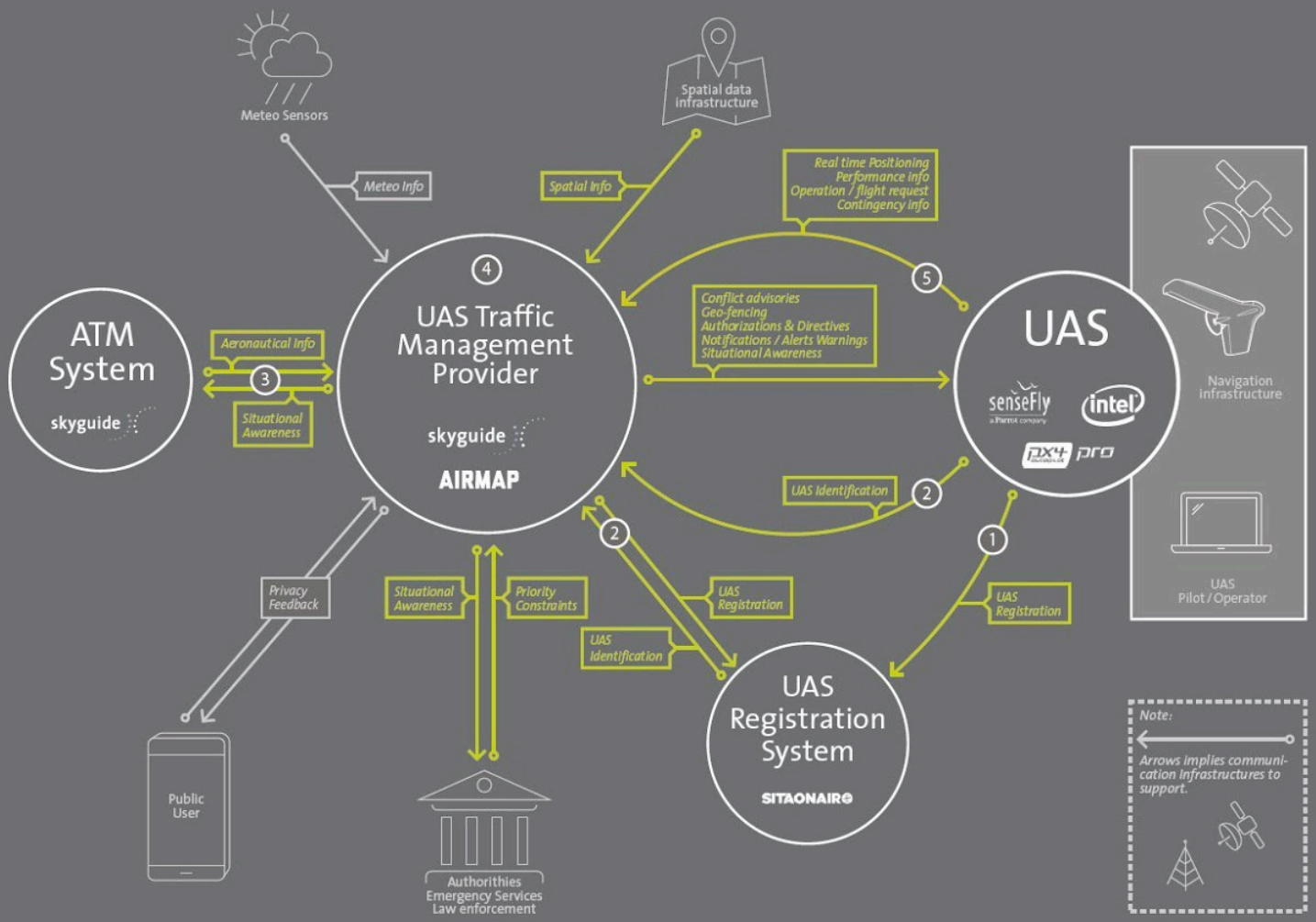

Add new Drone
Model
✓ Aerosense AS-DT01-E VTOL drone
Aerosense AS-MC01-P
DJI Agras MG-1
DJI Agras MG-1S
DJI Inspire 1
DJI Inspire 2
DJI Matrice 100
DJI Matrice 200
DJI Matrice 600
DJI Mavic Pro
DJI Mavic Pro Platinum
DJI Phantom 4
DJI Phantom 4 Advanced
DJI Phantom 4 Pro
DJI S1000+
DJI Spark
Flyability Elios
Intel Aero Ready-to-Fly drone
SenseFly albris
SenseFly eBee
SenseFly eBee Ag
SenseFly eBee Plus
SenseFly eBee RTK
SenseFly eBee SQ
Night
Nickname
Give your drone a nickname
Notes
Add drone


Radius:
900 ft
Ceiling:
800 ft/AFD
Centre:
46.2128112° N
6.1728611° E
Download map data
Mission Dates
Time Zone
Europe/Zurich
Start Date
14.09.2017
15:07
Now
Duration
30 mins
U-space
You are logged in.
Login
Flight
Drone ID: SUI-EVQ0XMZ8
Created
Drone ID
Approval
Air traffic
N/A
Create flight
Estimated Mission Wind
Mission Weather
D-01-27637
0 ft/ATO
1217 ft/AMSL
0:00
Idle
Ready for take-off
Quai de Cologny
Quai de Cologny
Quai de Cologny
Quai de Cologny
Rampe de

Drone pilot ground control station


Swiss-UAV-Lagrange_L...
Block
01_Corr-Gustave-...
Corridor Mapping
05:07
0.8 in/px
02_HMAP - Port Noir
Horizontal Mapping
10:09
0.8 in/px
25.8 acres
Add mission block
WARNING
HOME
START
HOLD
MISSION
MISSION
BLOCK
LAND
LANDING
ROLL
CLIMB
DESCENT
EP-00-015
14 ft/ATO
1229 ft/AMSL
0:00
GNSS status: RTK Fixed
Idle
Ready for take-off
Status
Idle
Ready for take-off
Autonomy
Battery
Flight time
Home distance
Link quality
Estimated wind
100 %
(12.5 V)
00:00
1 flight (15:57)
114 ft
(--:--)
95 %
(2.4 KB/s)
0.0 kts
Flight data
Ground speed: 0.0 kts
Altitude: 1229.2 ft/AMSL
Ground sensor height: -
Latitude: 46.2071204°
Longitude: 6.1651236°
Instruments
Temperature
Autopilot: 89.6°F
Camera: 78.8°F
GNSS
Satellites: 15 (46.8 dB/Hz)
Accuracy: 0.067 ft
Mode: RTK Fixed
Identification
Name: SUI-ZNDLODW6 (EP-00-015)
Drone Flight Log: EP-00-00015_0094.bb3
Camera information
Camera type: S.O.D.A. 1.2.0
Camera state: Standby
Number of photos: 0
External storage: 29.9 GB free of 29.9 GB
AS
kts
ALT
ft/ATO
Untertitel

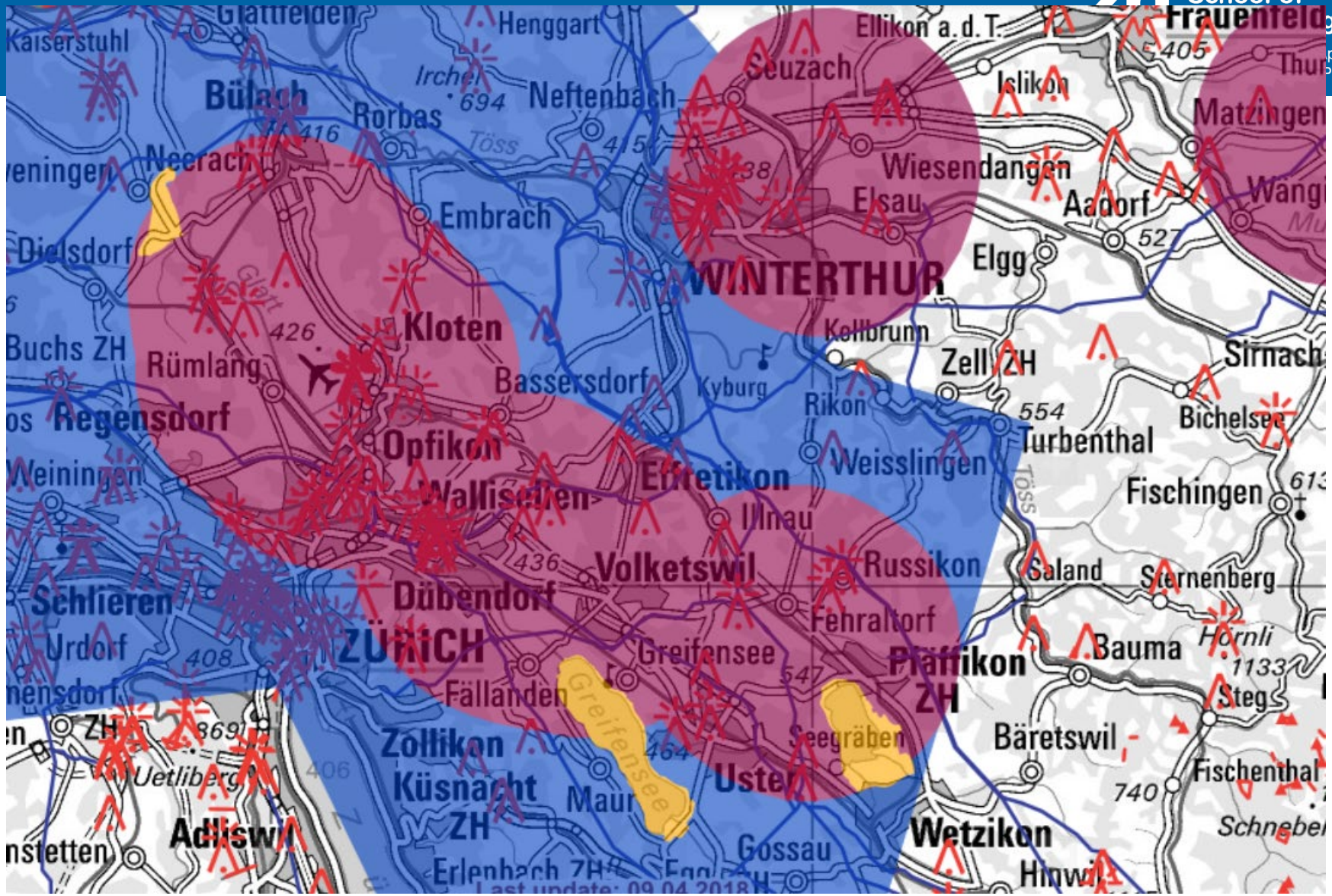
UTM Service Provider



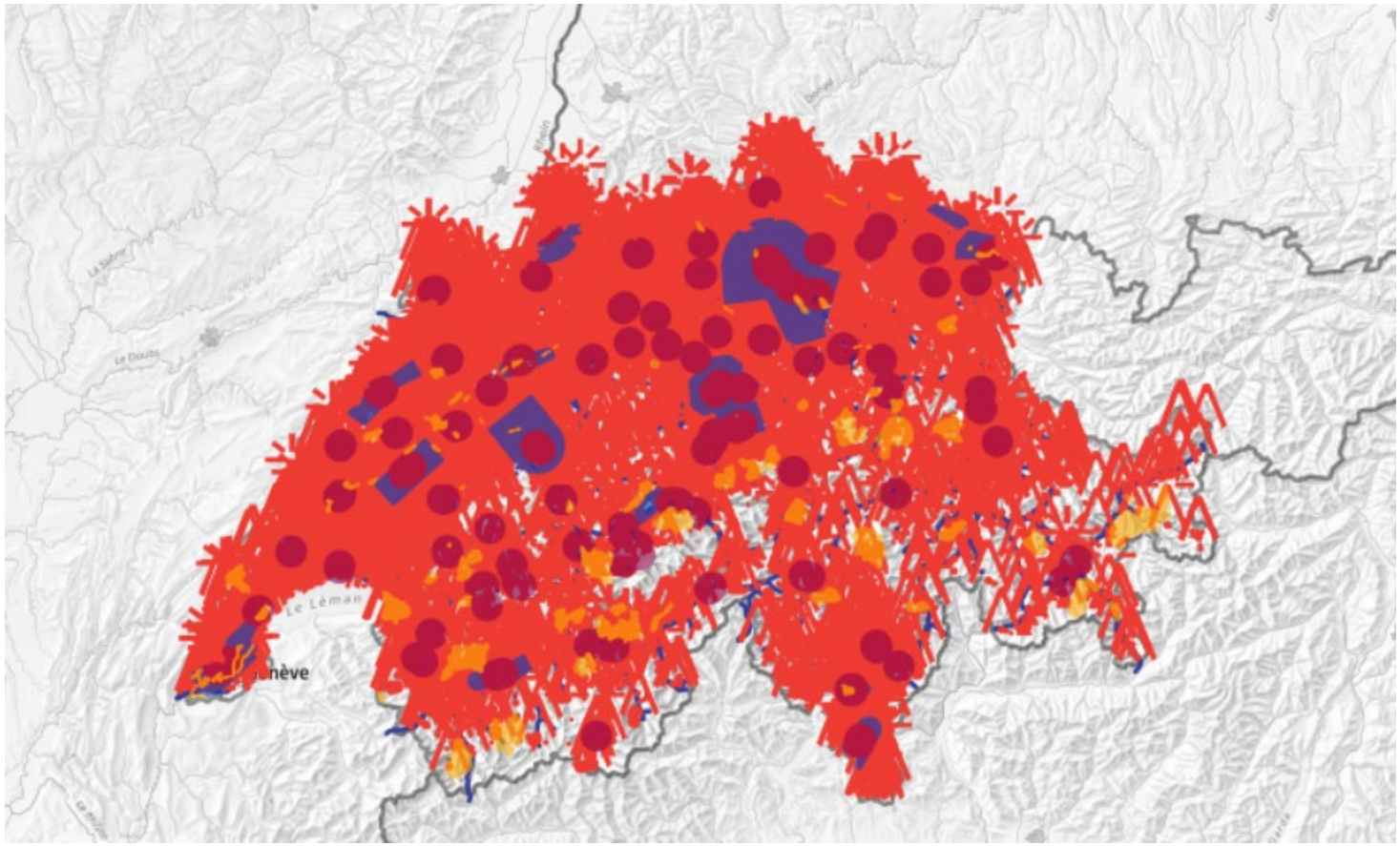
U-space in action

Skyguide and its project partners will demonstrate U1 and U2 capabilities including:

1. **Drone registration** with a Blockchain based database managed by SITAONAIR
2. **Authentication of the drone's identity** against the SITAONAIR registration database using AirMap technology
3. **Integration with ATC & digital airspace authorisation** from skyguide through the AirMap platform
4. **Dynamic flight plans and live telemetry** visualized on AirMap U-space dashboard
5. **Real-time drone telemetry data** sent by senseFly



Obstacle map and flight zone map by BAZL/ FOCA

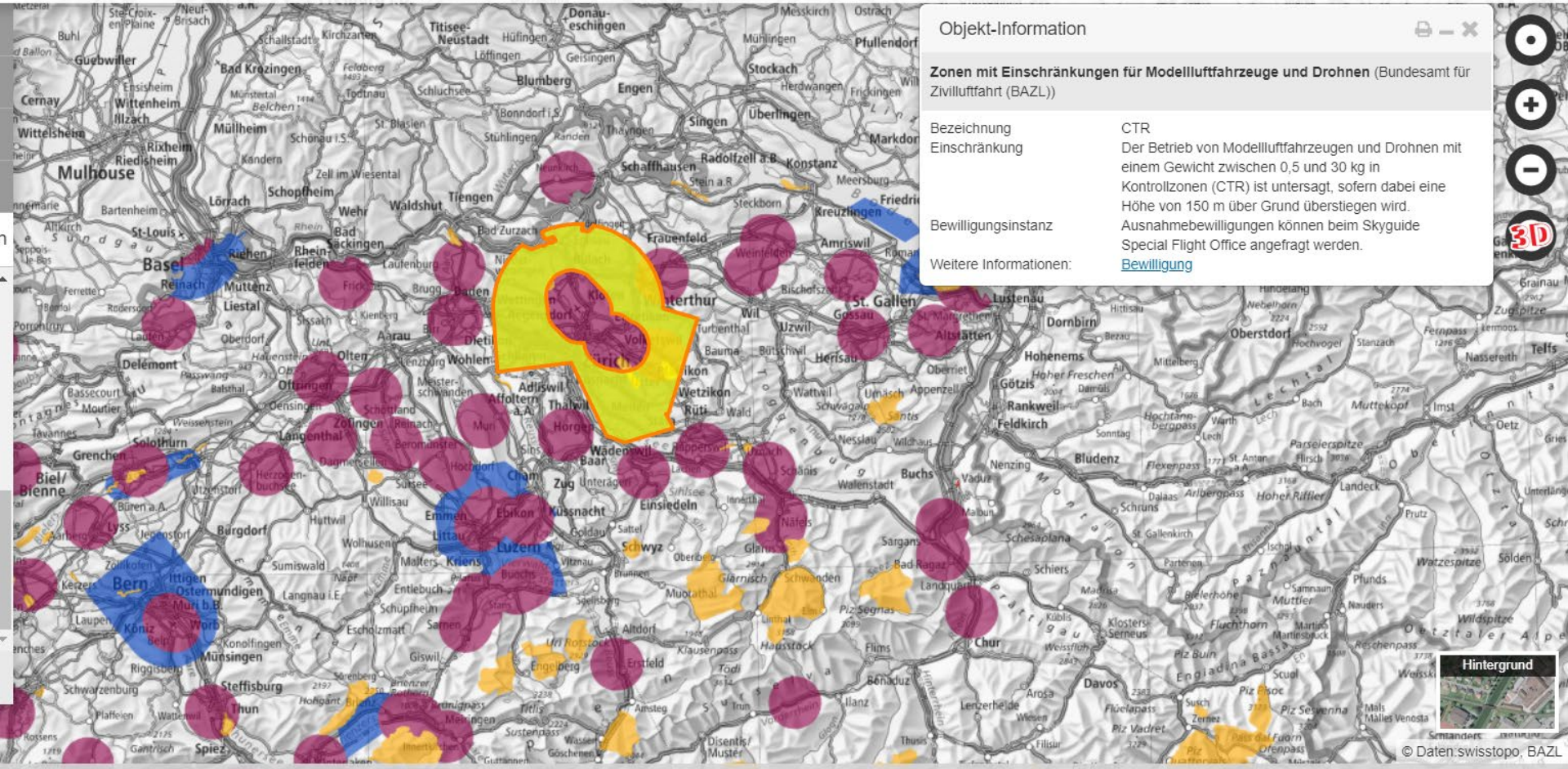


Obstacle map and flight zone map by BAZL/ FOCA

Ort suchen oder Karte hinzufügen:

z.B. Bundesplatz 1 Bern, 46.7 7.5, Lärmkarte ...

Vollbild Problem melden Hilfe Mobile Version DE FR IT EN RM



Datendownload Copyright & Datenschutzerklärung