A RESEARCH PERSPECTIVE ON SAFE AND CERTIFIABLE AUTONOMY

Johann Dauer, Institute of Flight Systems

ICAO RPAS Symposium, Montreal, November 7-9, 2022

DLR

# Flight Systems Research on RPAS / UAS

DLR at a glance

- Research institution
- Space administration
- Project management agency

Major research branches

- Aeronautics
- Space
- Energy
- Traffic
- Security
- Digitalisation

RPAS / UAS research at the Institute of Flight Systems

- Safe autonomy
- Artificial intelligence
- Environmental perception
- Guidance, navigation, control
- GNSS denied environments
- Safe operation
- Risk assessment
- Flight testing
- Methods for certification
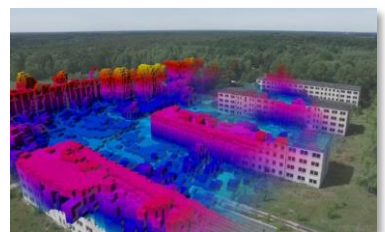
Autonomy
Emergence from Automation and Environment

Aircraft functions & components

Mission management & automation
Semantic environmental perception
Detect & avoid
Contingency & emergency management
System health management
Trajectory & motion planning
Trajectory optimization
Robust & fault-tolerant flight control
State and weather sensing

External Systems and Services

Airspace services (UTM / U-space)
Position systems
Datalink infrastructure

Levels of Autonomy

Human Involvement

Monitoring / responsibility
Procedures
Human factors
Crew qualification

Cooperation with other (autonomous) Systems

Transport infrastructure
Manned aviation
Ground / water vehicles

Risk-based Scaling the Assurance & Certification

Scaling the level of rigor and effort for certification:
Technical reliability (design and airworthiness, manufacturer, datalinks, maintenance, recovery)

→ Concept of Operations or Flight Manual as initial basis

passengers

full certification
New certification basis e.g. CS VTOL

air risk
(type of airspace /
traffic density)

ground risk
(kinetic energy /
population density)

© CC BY 4

minor airworthiness
requirements

operational risk based certification
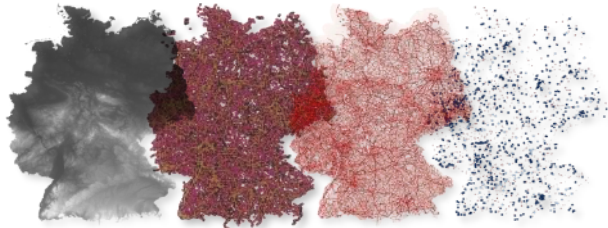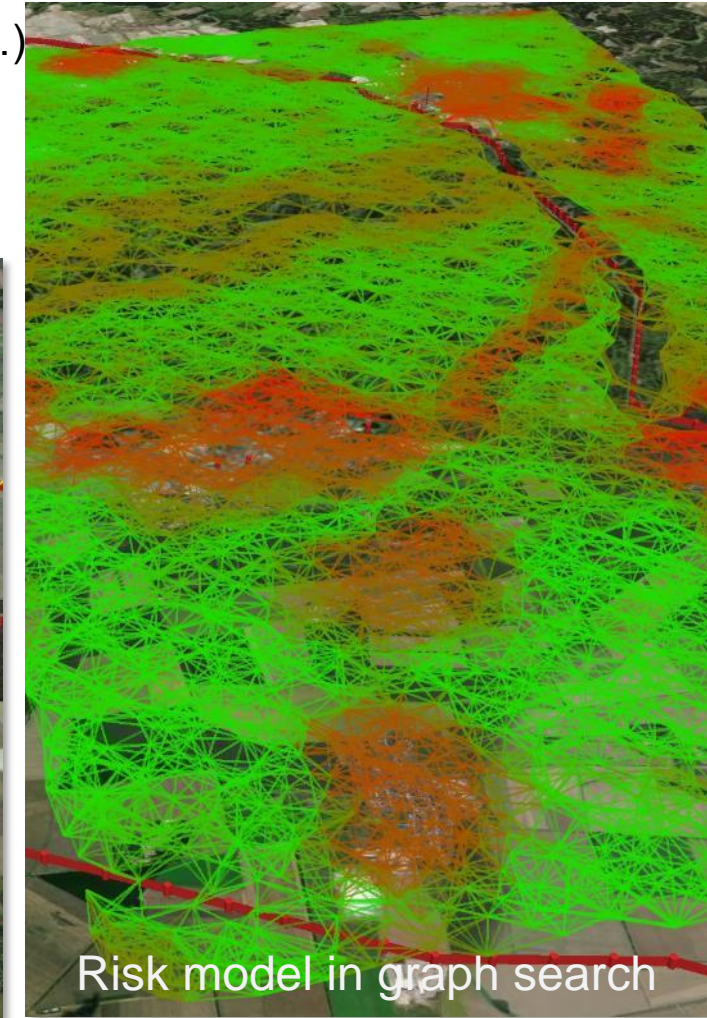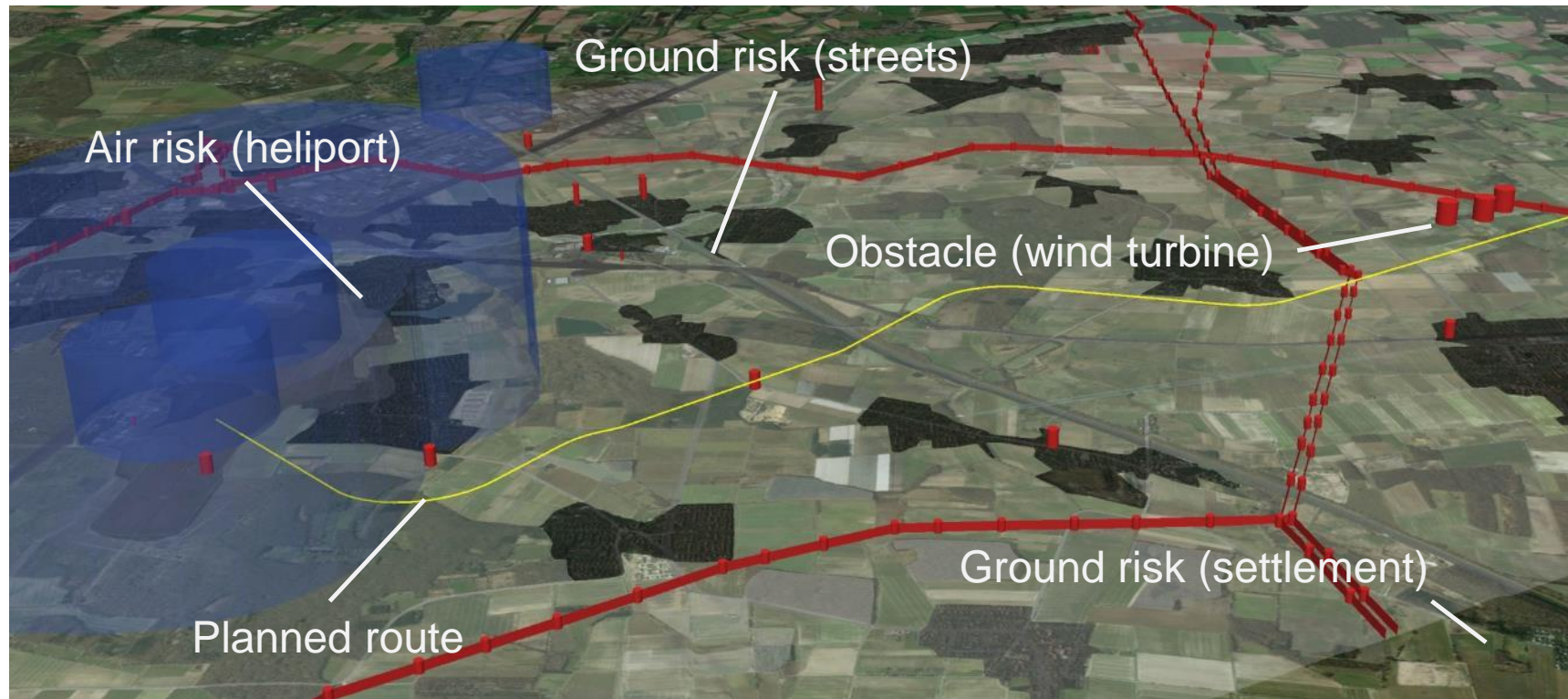**e.g. EASA's Specific Category: Specific Operations Risk**
Assessment(SORA)

4

Mapping Autonomy Functions to Operational Risks
Example: Risk-based Planning

- Layers of map information (traffic, land use, airspace …)
- Risk modelling for the operational volume
- Planning of routes with minimal operational risk
  ← → SORA

Air risk (heliport)

Ground risk (streets)

Obstacle (wind turbine)

Planned route

Ground risk (settlement)
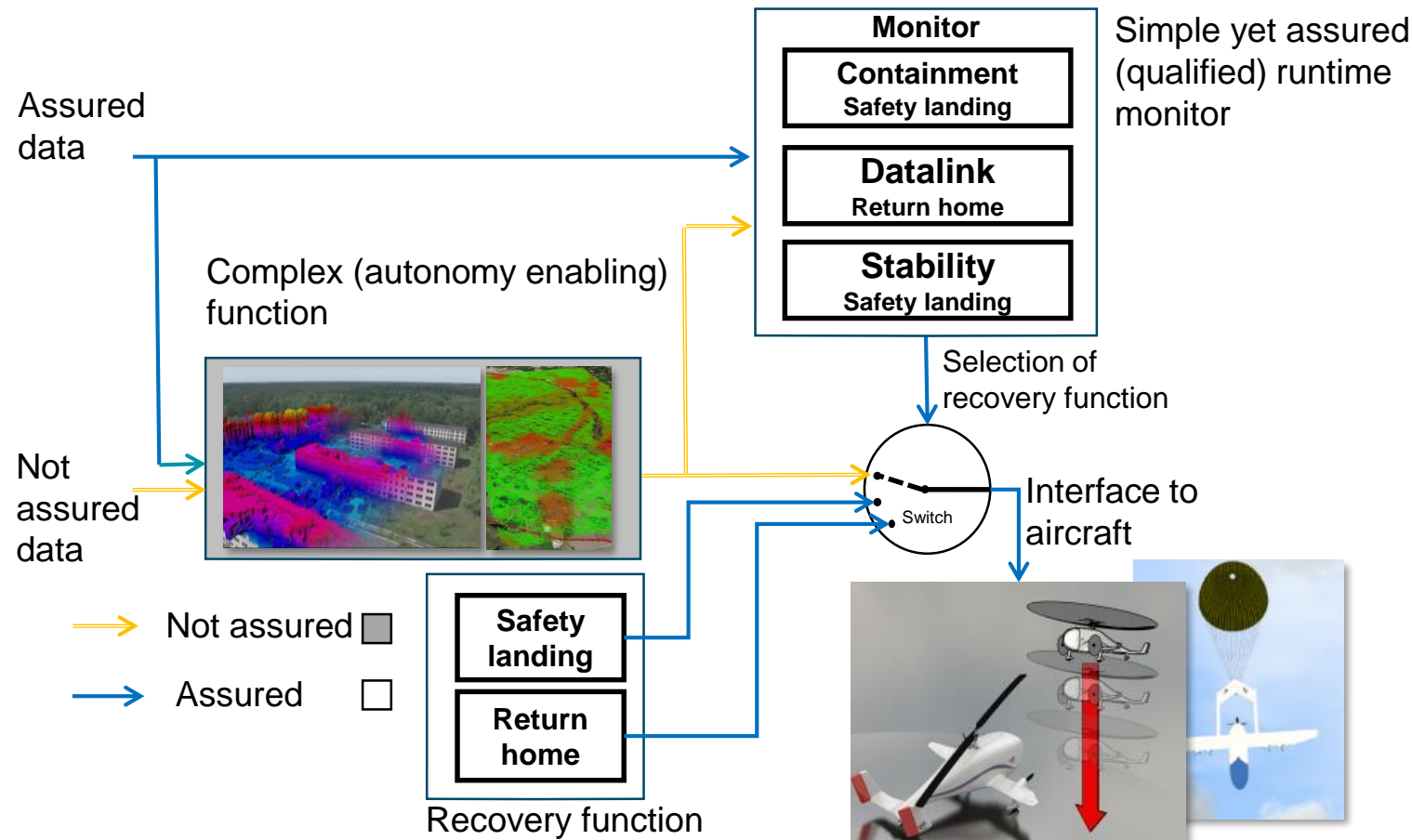
Risk model in graph search

Details: **Schopferer S, Donkels A** (2022) Trajectory risk modelling and planning for unmanned cargo aircraft. In: Automated Low Altitude Air Delivery. Springer, New York

Reducing the Certification Effort for Complex Function
Safe Operation Monitoring (Example Application of ASTM F3269)

Assured data

Complex (autonomy enabling) function

Not assured data

Monitor
- **Containment** — Safety landing
- **Datalink** — Return home
- **Stability** — Safety landing

Simple yet assured (qualified) runtime monitor

Selection of recovery function

Switch

Interface to aircraft

Not assured ☐
Assured ☐

Recovery function
- **Safety landing**
- **Return home**

Operational example:

- Flight in low risk flight corridor
- Safety landing / flight termination as contingency
- Supervision of operation to increase safety

Simulated geofence violation w. safety landing

Sensor status
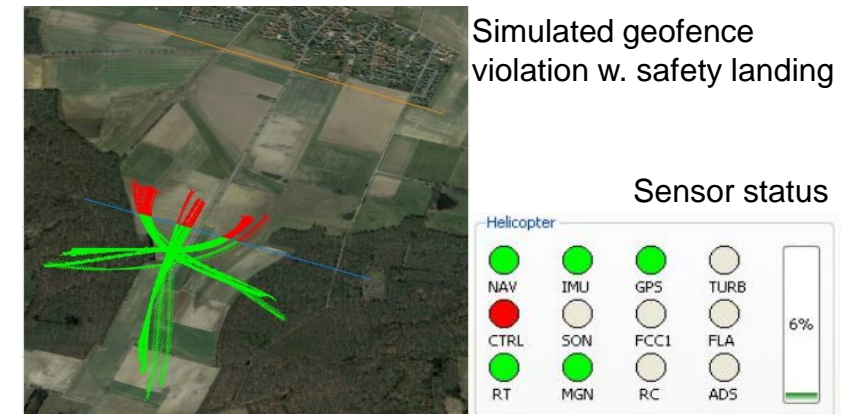
Automatic Contingency Management (ACM)
Handling the Unexpected

- Ideally ACM handles all unexpected events

- Challenges:
  - Comprehensive and reliable detection of critical situations
  - Comprehensive database of implemented (assured) recovery functions

- Complexity scales with operational risks

- Incremental build up of evidence. Starting with
  - With little operational risks
  - Sufficiently large defined margins
  - Small number of contingencies

- Automaton is thus one limiting factor of autonomy

Sensor inputs / System states → Runtime monitor → Contingency management → Mission management → Control commands
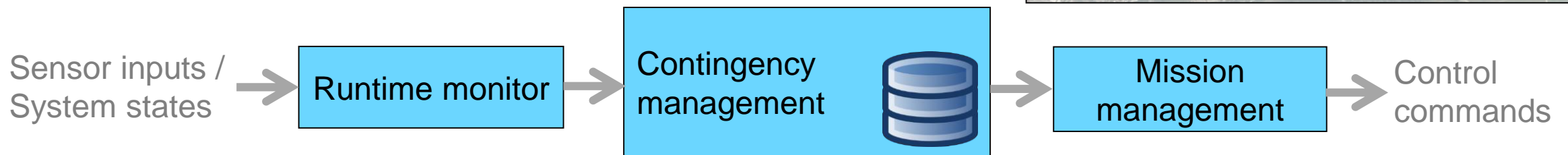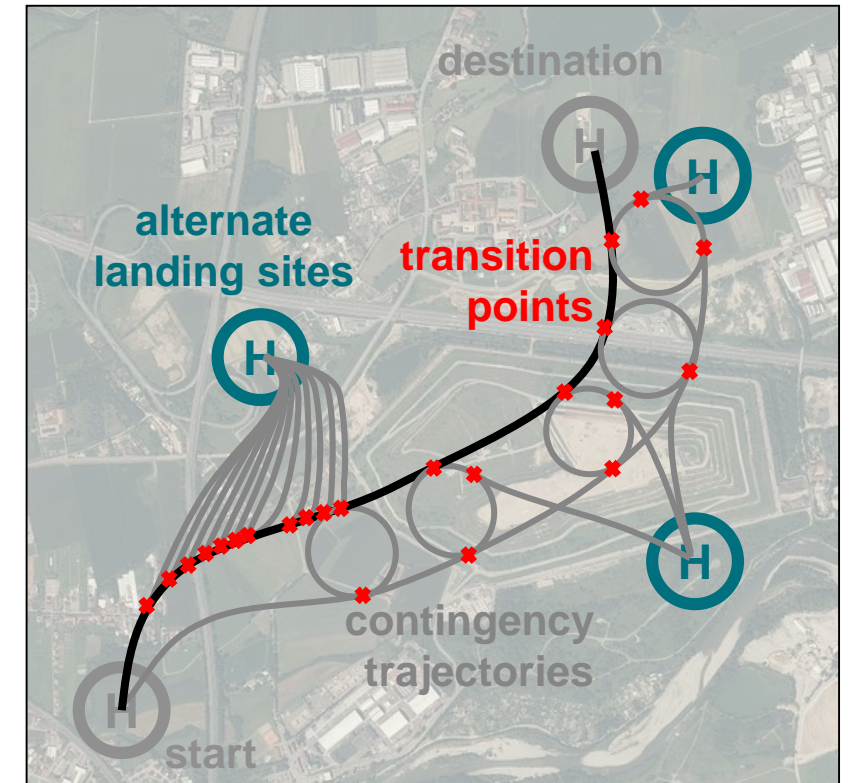
Looking Forward to Your Thoughts and Questions!
Get in Touch

Johann Dauer
Mail: johann.dauer@dlr.de
Phone: +49 531 295 3262

Department of Unmanned Aircraft
Institute of Flight Systems
Lilienthalplatz 7, 38108
Braunschweig, Germany