Formal verification of small and micro UAS

Prof Sandor M Veres
University of Sheffield

December 2, 2015

The purpose of my talk

- Addressing the problem of verifying autonomous operations of UAS engineering systems in various type of environments such as enclosed areas, congested areas, over countryside under 400ft and in national airspace are considered.

The purpose of my talk

- Addressing the problem of verifying autonomous operations of UAS engineering systems in various type of environments such as enclosed areas, congested areas, over countryside under 400ft and in national airspace are considered.
- What to verify? What are the requirements? How to verify?

The purpose of my talk

- Addressing the problem of verifying autonomous operations of UAS engineering systems in various type of environments such as enclosed areas, congested areas, over countryside under 400ft and in national airspace are considered.
- What to verify? What are the requirements? How to verify?
- Identify models which are general enough to be applicable to most practical autonomous UAS and their subsystems.

What to Verify?

- The UAS is assumed to be in operation in various environmental scenarios

What to Verify?

- The UAS is assumed to be in operation in various environmental scenarios
- What does verification mean for this engineering system?

What to Verify?

- The UAS is assumed to be in operation in various environmental scenarios
- What does verification mean for this engineering system?
- The challenge is to ascertain that it will function in materially and legally acceptable manner with high probability

What to Verify?

- The UAS is assumed to be in operation in various environmental scenarios
- What does verification mean for this engineering system?
- The challenge is to ascertain that it will function in materially and legally acceptable manner with high probability
- We need to make the definition of UAS verification more precise

What to Verify?

- The UAS is assumed to be in operation in various environmental scenarios
- What does verification mean for this engineering system?
- The challenge is to ascertain that it will function in materially and legally acceptable manner with high probability
- We need to make the definition of UAS verification more precise
- What are the methods available to achieve verification and what is missing?

What are the models and requirements?

- Joint autopilot and aircraft dynamics in closed loop. (APD)

What are the models and requirements?

- Joint autopilot and aircraft dynamics in closed loop. (APD)
- Broad set of environmental models for the legal airspace, concerning weather conditions and presence of other aircraft, buildings and variations of terrain on the ground. (LAS)

What are the models and requirements?

- Joint autopilot and aircraft dynamics in closed loop. (APD)
- Broad set of environmental models for the legal airspace, concerning weather conditions and presence of other aircraft, buildings and variations of terrain on the ground. (LAS)
- Effectiveness of perception/sensory systems under all environmental conditions. (PEN)

What are the models and requirements?

- Joint autopilot and aircraft dynamics in closed loop. (APD)
- Broad set of environmental models for the legal airspace, concerning weather conditions and presence of other aircraft, buildings and variations of terrain on the ground. (LAS)
- Effectiveness of perception/sensory systems under all environmental conditions. (PEN)
- Situational awareness under all environmental conditions and possible damage to the aircraft itself. (SAE)

What are the models and requirements?

- Joint autopilot and aircraft dynamics in closed loop. (APD)
- Broad set of environmental models for the legal airspace, concerning weather conditions and presence of other aircraft, buildings and variations of terrain on the ground. (LAS)
- Effectiveness of perception/sensory systems under all environmental conditions. (PEN)
- Situational awareness under all environmental conditions and possible damage to the aircraft itself. (SAE)
- Legally transparent decision making system onboard, including planning and path planning . (LTD)

What are the models and requirements?

- Joint autopilot and aircraft dynamics in closed loop. (APD)
- Broad set of environmental models for the legal airspace, concerning weather conditions and presence of other aircraft, buildings and variations of terrain on the ground. (LAS)
- Effectiveness of perception/sensory systems under all environmental conditions. (PEN)
- Situational awareness under all environmental conditions and possible damage to the aircraft itself. (SAE)
- Legally transparent decision making system onboard, including planning and path planning . (LTD)
- Redundant and distributed computation and sensor/actuator systems to safeguard against most likely hardware failures. (DCS)

Outline of the UAS Verification Process

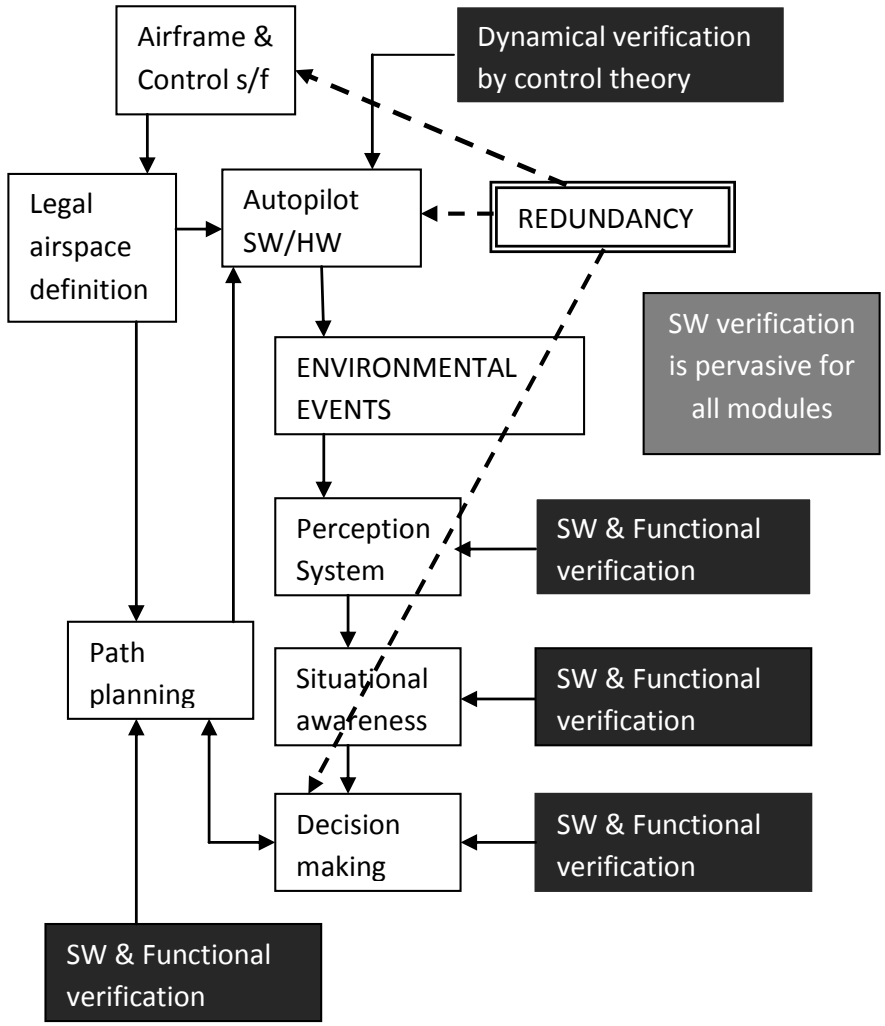

Figure: Sub-problems of functional verification of UAS

Requirement for Autopilot & Dynamics

- The most studied problem for safety of aircraft is the safety of its control systems to make it fly under varied weather conditions.

Requirement for Autopilot & Dynamics

- The most studied problem for safety of aircraft is the safety of its control systems to make it fly under varied weather conditions.
- This has been the focus of manned aircraft design for the last six decades.

Requirement for Autopilot & Dynamics

- The most studied problem for safety of aircraft is the safety of its control systems to make it fly under varied weather conditions.
- This has been the focus of manned aircraft design for the last six decades.
- Research and methods of manned aviation to secure safety should not be ignored for UAS

Requirement for Autopilot & Dynamics

- The most studied problem for safety of aircraft is the safety of its control systems to make it fly under varied weather conditions.
- This has been the focus of manned aircraft design for the last six decades.
- Research and methods of manned aviation to secure safety should not be ignored for UAS
- Often more threat to the environment than to the vehicle if it is inexpensive.

Requirement for Autopilot & Dynamics

- The most studied problem for safety of aircraft is the safety of its control systems to make it fly under varied weather conditions.
- This has been the focus of manned aircraft design for the last six decades.
- Research and methods of manned aviation to secure safety should not be ignored for UAS
- Often more threat to the environment than to the vehicle if it is inexpensive.
- Need for suitable legal frameworks, potentially a global one, for UAS aviation rules.

System models for Autopilot & Dynamics

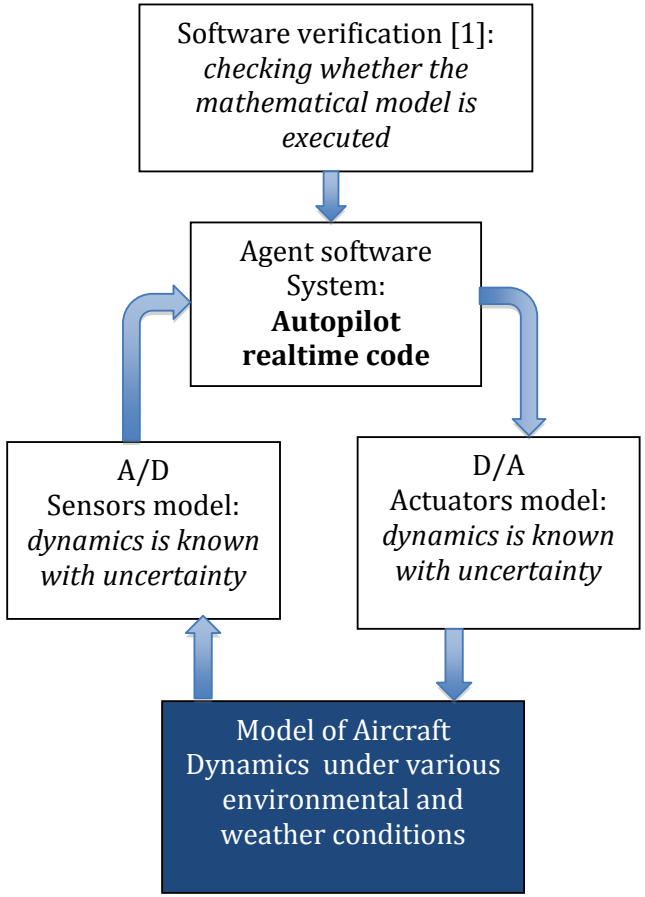

Figure: Verification of UAS models and the environment with uncertainty.

System models for Autopilot & Dynamics

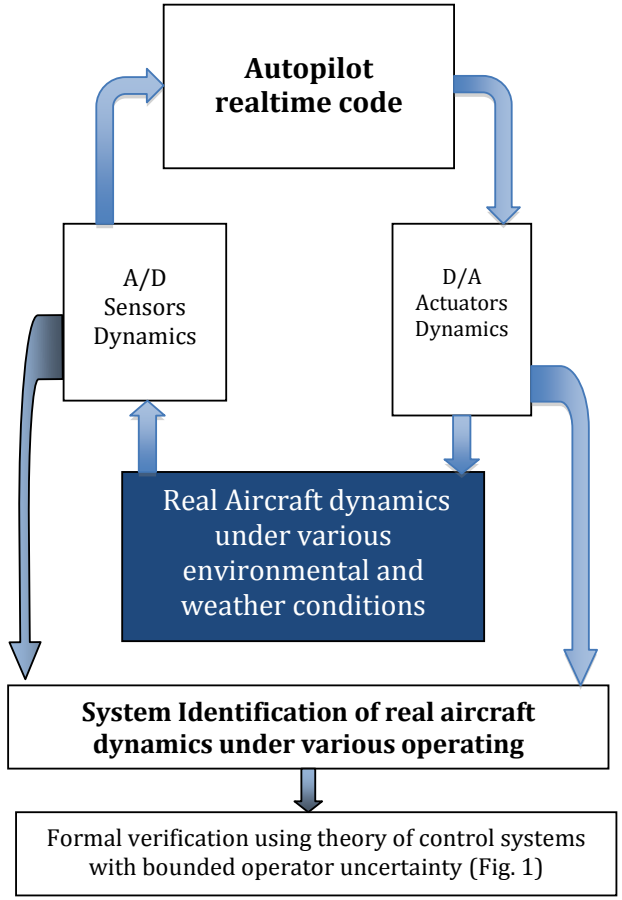

Figure: System Identification (SysId) of real aircraft dynamics under various operating conditions to support formal verification.

Legal Definitions of Airspaces - LAS

- Each type of UAS is subject to different regulation with regard to where it is permitted to fly, dependent on its weight, payload and prevailing weather conditions.

Legal Definitions of Airspaces - LAS

- Each type of UAS is subject to different regulation with regard to where it is permitted to fly, dependent on its weight, payload and prevailing weather conditions.
- Legal airspaces may be defined in a number of ways such as geographic regions (e.g. Aerodrome Traffic Zones) or relative boundaries (e.g. proximity to people) and may impose restrictions on the operation.

Legal Definitions of Airspaces - LAS

- Each type of UAS is subject to different regulation with regard to where it is permitted to fly, dependent on its weight, payload and prevailing weather conditions.
- Legal airspaces may be defined in a number of ways such as geographic regions (e.g. Aerodrome Traffic Zones) or relative boundaries (e.g. proximity to people) and may impose restrictions on the operation.
- During verification, it is necessary to expose the UAS to all combinations of legal airspaces it may encounter to verify its performance.

Legal airspace based on UAS class and environment

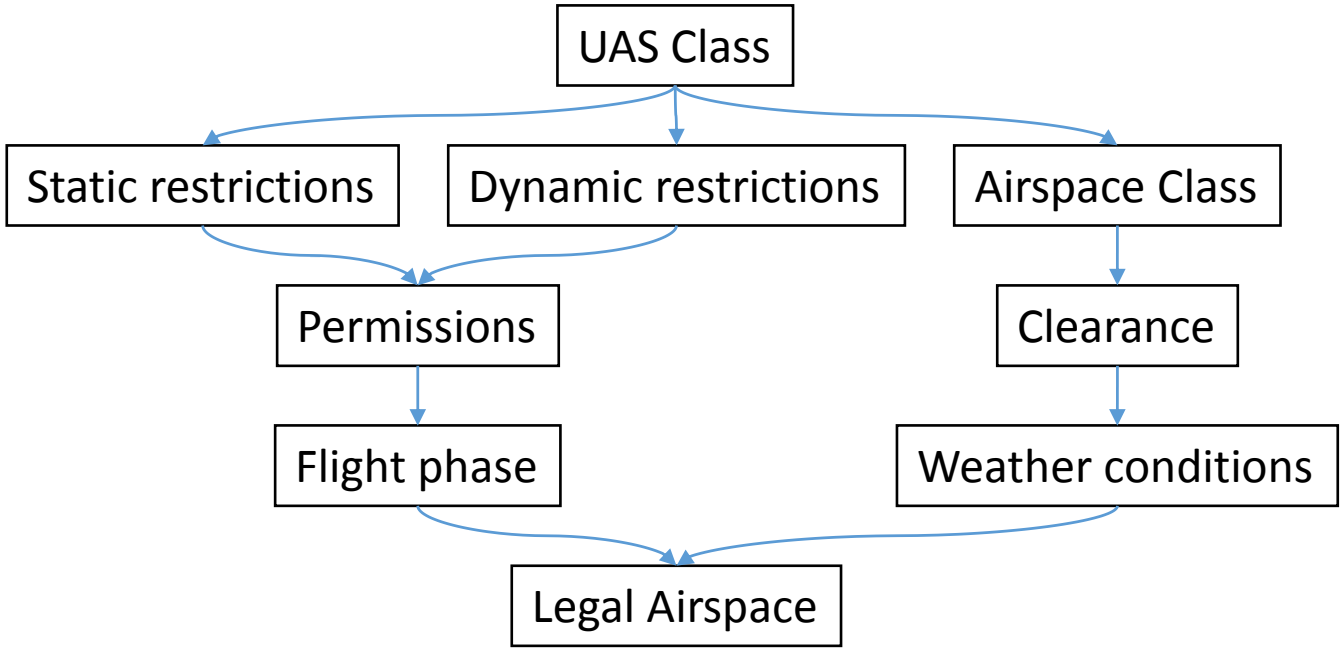

Figure: Determination of legal airspace based on UAS class and operating environment

Environmental perception system onboard a UASt

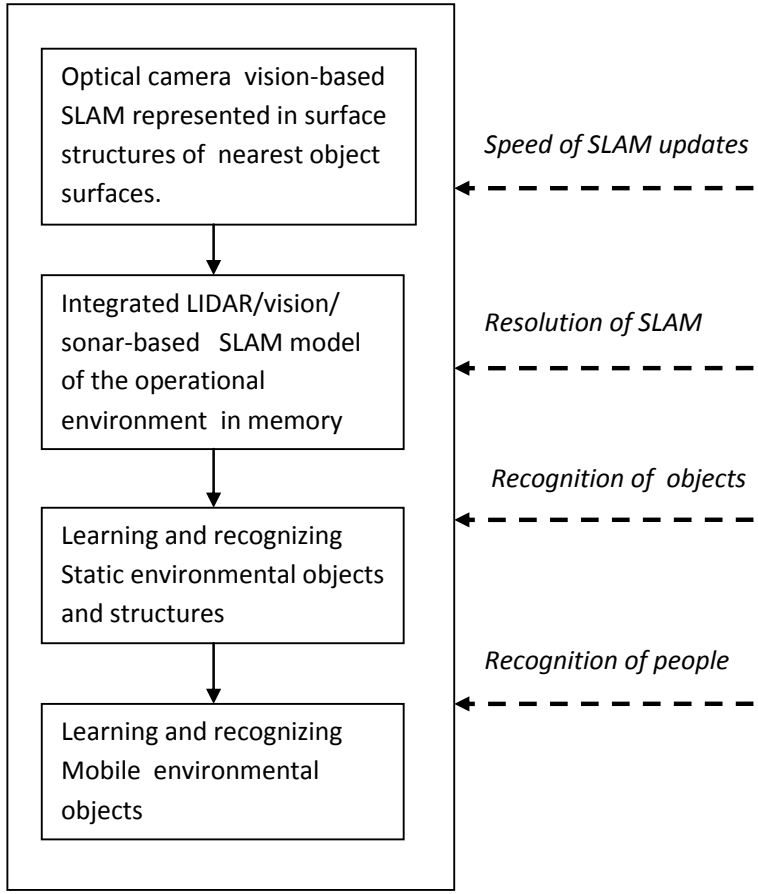

Figure: The environmental perception system onboard a UAS to be verified.

Quality of computer vision systems

- Efficient estimation of disparity statistics has been used as a predictor for perceived 3D video scene quality

Quality of computer vision systems

- Efficient estimation of disparity statistics has been used as a predictor for perceived 3D video scene quality
- A good quality stereo pair is a precondition of 3D modelling of the environment.

Quality of computer vision systems

- Efficient estimation of disparity statistics has been used as a predictor for perceived 3D video scene quality
- A good quality stereo pair is a precondition of 3D modelling of the environment.
- Mono cameras can also be used almost equally to stereo cameras. The exception is when the drone is hovering still and approach of other objects needs to be estimated.

Quality of computer vision systems

- Efficient estimation of disparity statistics has been used as a predictor for perceived 3D video scene quality
- A good quality stereo pair is a precondition of 3D modelling of the environment.
- Mono cameras can also be used almost equally to stereo cameras. The exception is when the drone is hovering still and approach of other objects needs to be estimated.
- One of the remaining challenges of autonomous UAS is to produce *methods for realtime 3D dense environmental models* (REDEM)

Quality of computer vision systems

- Efficient estimation of disparity statistics has been used as a predictor for perceived 3D video scene quality
- A good quality stereo pair is a precondition of 3D modelling of the environment.
- Mono cameras can also be used almost equally to stereo cameras. The exception is when the drone is hovering still and approach of other objects needs to be estimated.
- One of the remaining challenges of autonomous UAS is to produce *methods for realtime 3D dense environmental models* (REDEM)
- A second challenge is the *camera movement requirements* to ensure a complete REDEM in realtime.

The role of knowledge in perception

Recognition of other aerial vehicles and to interpret their purpose is important for a UAS to make decisions. For instance:

- Emergency by aircraft normally flying higher than 500ft
- Take off or landing of manned aircraft
- Police an other emergency services using manned helicopter or UAS
- In airspace over non-congested areas such as countryside, agricultural UAS or other UAS on security patrol.
- In all areas UAS use for leisure.
- etc.

Quality of dense scene reconstruction

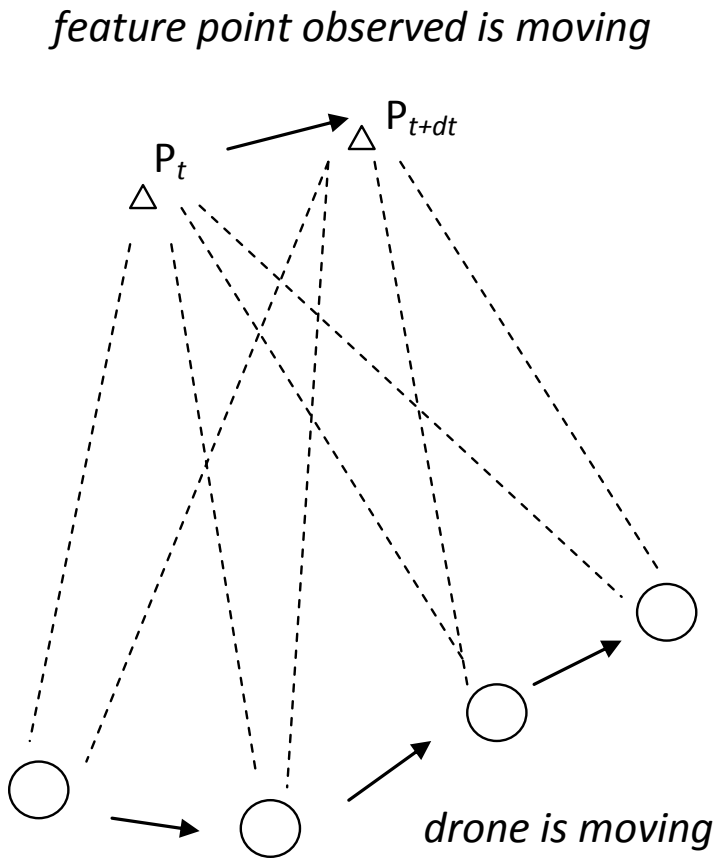

Figure: Multiple view of the same spatial points are needed for secure detection in sense and avoid.

Multi-sensor detection

- Large homogeneous surfaces in the surround will be difficult to match in images for structure from motion algorithms.
- Complementary method of using lidar to explore these homogeneous regions can resolve the remaining ambiguity.
- Ultrasonic sensors and be also activated to detect difficult to see nearby object
- Verifiable sense and avoid the Vision-Lidar-Ultrasonics (VLU) based adaptive "sense and avoid" system needs to operate in all directions in a 3D coordinate system centred at the UAS

Omnidirectional detection is needed

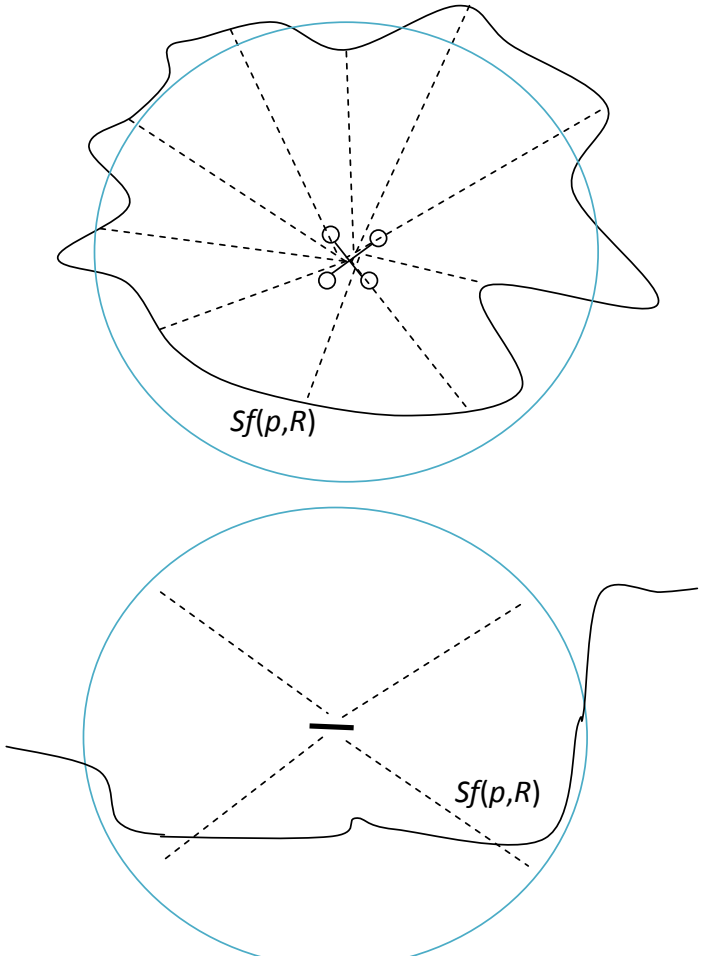

Figure: The environmental perception system onboard a UAS to be verified.

Formal description of omnidirectional detection

Let define spherical polar coordinate system centred at location p of the UAS by

$$S(p) = \{(a, e, r) : a \in [-\pi, \pi], e \in [-\pi/2, \pi/2], r \geq 0\}$$

and associated sphere of the sense and avoid space by

$$S(p, R) = \{(a, e, r) \in S(p) : r \leq R\}$$

The detected environmental surface with $S(p, R)$ is

$$Sf(p, R) = \{(a, e, \rho) \in S(p, R) : (a, e, [0, \rho) \text{ is free space}$$

$$\text{and}(a, e, \rho) \text{ is a surface point on an object or } \rho = R\}$$

The velocity vectors of detected environmental objects defined by:

$$Mf(p, R) = \dot{S}f(p, R) - \dot{p}$$

Formal description of omnidirectional detection

Proposition 1. A UAS' sense and avoid perceptions (SAAP) system is formally verifiable to be equivalent to the perception of a human pilot (or or exceeding it in performance) if the SAAP provides full spherical coverage of $Sf(p_t, R)$ and $Mf(p_t, R)$ at all times t during flight within a time delay less than dt which legally describes human reaction time (of the human visual system) and $R > 0$ defines legally acceptable range of human visual perception.

Three levels of situation awareness

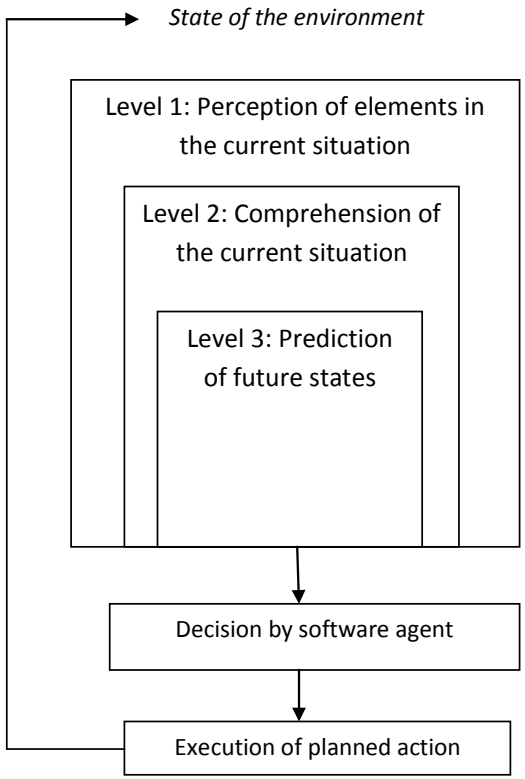

Figure: Three levels of situation awareness within an autonomous UAS

Situational Awareness of the Environment - SAE

- Builds on verified perception system
- Comprehension and prediction, which assign meaning to the perceived elements
- Predict their future states of the environment. For instance, when perceiving a potential collision risk, it is this projected state information which is most useful to the UAS' decision making system when taking evasive action.
- Statistical models which capture both the expected behaviour and their uncertainty
- UAS should be given some preliminary models and the freedom to learn new ones and refine them over time
- This is a new challenge of *learning situational awareness* for verifying and certifying future AUAS.

Coverage directed generation of situations

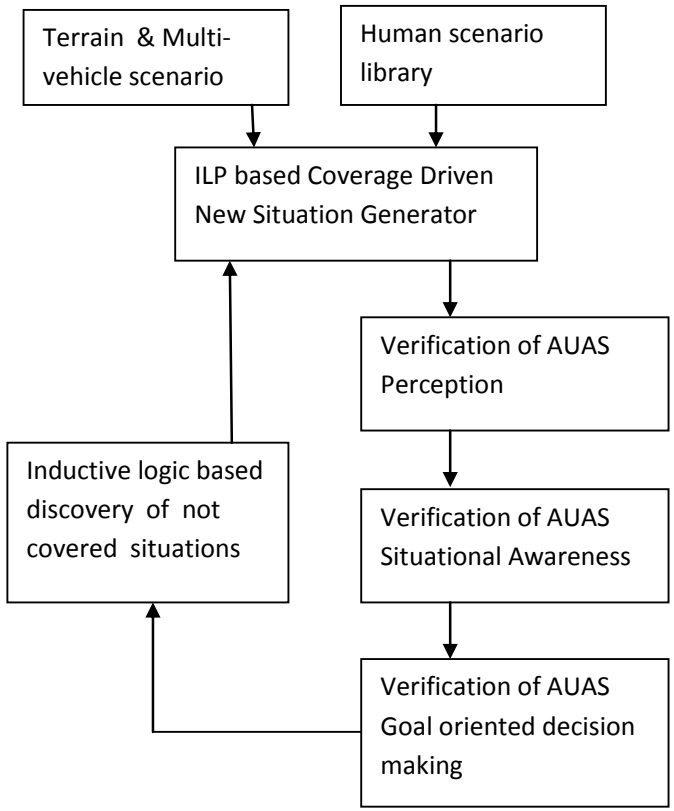

Figure: Coverage directed generation of situations for verification by K. Eder

Verification of decision making

- Situational awareness creates the abstractions of current situations and situation which will rapidly develop for the AUAS and it must take them into account in its decision.
- Constraints of future events can be applied both by planner based decision making as well as by rational agent decisions
- Use of the SPIN model checker o verify a UAS decision systems (Webster, Fisher). UAS' decision making system when taking evasive action.
- Agent-based autonomous control system verified using Agent Java Path Finder (AJPF) (Dennis et al.)
- Use of abstracted virtual environments (Cameron et al.)
- Runtime verification - verification carried out by the UAS to ascertain its decisions.

Redundant and Distributed Computation - DCS

There are a number of possibilities for physical duplication of components for safety, for UAS the most relevant ones are:

- multiplication of the autopilot hardware including IMU and pressure sensors (2-3)
- multiplication of the SLAM processor for perception
- multiplication of the SA processor for situational awareness
- multiplication of decision making processor for mission objectives

Conclusions 1-3

- APD - Autopilot verification. The manned aircraft industry provides basic methodologies. A remaining challenge is to make this process inexpensive. The prospects for this are today very good due to two reasons: developments in system identification of nonlinear bounded-uncertainty aircraft dynamical models and robust control methods in combination with agent supervised autopilot training onboard a UAS.

Conclusions 1-3

- APD - Autopilot verification. The manned aircraft industry provides basic methodologies. A remaining challenge is to make this process inexpensive. The prospects for this are today very good due to two reasons: developments in system identification of nonlinear bounded-uncertainty aircraft dynamical models and robust control methods in combination with agent supervised autopilot training onboard a UAS.
- LAS - Legal airspace environmental conditions. Virtual reality simulation models have developed a lot recently. These combined with abstractions of conditions can serve the basis for coverage driven formal analysis of AUAS response.

Conclusions 1-3

- APD - Autopilot verification. The manned aircraft industry provides basic methodologies. A remaining challenge is to make this process inexpensive. The prospects for this are today very good due to two reasons: developments in system identification of nonlinear bounded-uncertainty aircraft dynamical models and robust control methods in combination with agent supervised autopilot training onboard a UAS.
- LAS - Legal airspace environmental conditions. Virtual reality simulation models have developed a lot recently. These combined with abstractions of conditions can serve the basis for coverage driven formal analysis of AUAS response.
- PEN - Perception of the environment. Computer vision has developed considerably during the past few years and we are now near to achieving realtime dense scene perception.

Conclusions 4-5

- SAE - Situational awareness of the environment. Machine knowledge representations, which are compatible both with rational agent software as well as are human readable and hence legally adoptable, are now available and can facilitate descriptions of rules of the air as well as making agents learn by example during their operations.

Conclusions 4-5

- SAE - Situational awareness of the environment. Machine knowledge representations, which are compatible both with rational agent software as well as are human readable and hence legally adoptable, are now available and can facilitate descriptions of rules of the air as well as making agents learn by example during their operations.
- LTD - Legally transparent decision making system onboard. If agent decision making were described in English, which would compile into the decision making system of agents controlling an AUAS, that would make this feasible. Such a system is now available and needed to be applied to verifiable autonomous UAS.

Conclusions 4-5

- SAE - Situational awareness of the environment. Machine knowledge representations, which are compatible both with rational agent software as well as are human readable and hence legally adoptable, are now available and can facilitate descriptions of rules of the air as well as making agents learn by example during their operations.
- LTD - Legally transparent decision making system onboard. If agent decision making were described in English, which would compile into the decision making system of agents controlling an AUAS, that would make this feasible. Such a system is now available and needed to be applied to verifiable autonomous UAS.
- SWV - Verification of all software correctness. This is needed in order to check that the mathematical definitions of what the software should do and what the code actually does, do match. Methods are available to do this for robot navigation and control,.

References

[1] H. Xia and S. M. Veres, Improved efficiency of adaptive robust control by model unfalsification, Automatica, vol. 35, no. 5, pp. 981? 986, 1999.
[2] S. M. Veres and D. S. Wall, Synergy and Duality of Identification and Control. London: Taylor & Francis, 2000.
[3] S. Tantrairatn and S. M. Veres, A rational agent framework for adaptive flight control of UAV, ICUAS'15, International Conference on Unmanned Aircraft Systems June 9-12, Denver Marriott Tech Center, 2015.
[4] O. McAree, Autonomous terminal area operations for unmanned aerial systems, Ph.D. dissertation, Loughborough University, 2013.
[5] K. Eder, P. Flach, and H.-W. Hsueh, Fowards automating simulation- based design verification using ILP, LNAI 4455, Springer, vol. 33, pp. 154?168, 2007.

References

[6] Autonomous Asteroid Exploration by Rational Agents, by Lincoln, Veres, et al. IEEE Computational Intelligence Magazine Vol. 8, No 4, pp 25-38, 2013
[7] On Efficient Consistency Checks by Robots, by Hongyang Qu and Sandor M Veres , The European control Conference, 2014
[8] *Natural Language Programming of Agents and Robotic Devices* (book), S M Veres, SysBrain, London, 2008
[9] Formal methods for the certification of autonomous unmanned aircraft systems, Iby M. Webster, M. Fisher et al, In Computer Safety, Reliability, and Security, 2011, pp. 228-242.
[10] Knowledge of machines: review and forward look, by S. M. Veres, Proc. IMechE Vol. 225 Part I: J. Systems and Control Eng., pp. 1-8, 2015.

Thank you for your attention

Any more questions?