UxAS Requirement Sheet

# Summer of Innovation, Requirements Team

Air Force Research Laboratory, Wright Brothers Institute, Summer 2017

## General

1. A **reusable framework** is needed that must support a broad class of autonomous ISR missions using unmanned assets —  including unmanned aircraft.
2. The framework must enable **distributed**, multi-agent **cooperative control** in a comms-denied environment.
3. The framework must be **modular**
4. The framework must be **computationally efficient**
5. The framework must run on modest hardware
6. ~~The framework must allow capabilities such as~~ **~~mission planning~~**~~, path planning, and surveillance tasks to be~~ **~~efficiently developed~~** ~~and rapidly updated and replaced before the start of each ISR mission.~~
7. The framework must allow for **mission planning** tasks
8. The framework must allow for **path planning** tasks
9. The framework must allow for **mission planning** tasks
10. The framework must allow for tasks to be efficiently developed, rapidly updated, and rapidly replaced before the start of ISR missions.
11. The framework must optimize tasks for mission-time efficiency.
12. The framework must ensure **safety** and **security**.
13. The framework must facilitate **formal verification and validation**.

## Reviewed/Consolidated Reqs

1. UxAS shall enable cooperative control.
2. UxAS shall support multiple agents.
3. UxAS shall be distributed.
4. UxAS shall operate when there is no comms.
5. UxAS shall operate in the presence of lost comms
6. UxAS shall operate in the presence of denied comms
7. UxAS shall be modular
8. UxAS shall be computationally efficient; to run quickly on cell-phone sized processors
9. UxAS will run on modest hardware, e.g., cell-phone sized processor
10. UxAS shall allow tasks to be efficiently developed
11. ~~Example tasks include mission planning, path planning, and surveillance~~
12. UxAS shall allow configurations to be rapidly modified before the start of a mission
13. ~~Configuration modification includes task update before the start of each mission~~
14. ~~update may mean that the component satisfies its contract in a new way~~
15. ~~Configuration modification includes task replacement before the start of a mission~~
16. ~~replace may mean that the contract has been changed and the configuration needs to be re-analyzed~~
17. Configurations shall optimize tasks for mission-time efficiency
18. ~~Configurations shall ensure the safety of agents~~
19. Configurations shall ensure the safety of agents by having collision avoidance.
20. Configurations shall ensure the safety of agents by having health monitoring.
21. Configurations shall ensure the safety of agents by having contingency planning
22. ~~Safety includes collision avoidance, health monitoring, contingency planning (safe route home for lost comms)~~
23. ~~Configurations shall ensure security~~
24. Configurations shall ensure security integrity & confidentiality of comms
25. Configurations shall ensure security integrity & confidentiality of onboard data
26. Configurations shall ensure security availability of computing resources
27. ~~Security includes integrity & confidentiality of comms~~
28. ~~Security includes integrity & confidentiality of onboard data~~
29. ~~Security includes availability of computing resources~~
30. UxAS shall facilitate formal verification and validation
31. UxAS shall be employ a service-oriented architecture
32. Configurations shall be based off of a service oriented architecture
33. Configurations shall ensure schedulability of tasks
34. Configurations shall ensure timeliness of task execution
35. Configurations shall ensure timeliness of message delivery within an asset
36. Configurations shall guarantee non-interference amongst services under nominal hardware configurations
37. Configurations shall provide time partitioning of services
38. Configurations shall provide space partitioning of services
39. Configurations shall provide resource partitioning of services
40. ~~For example, configurations will schedule direct-memory access~~
41. Configurations shall provide a message-passing interface for inter-service communication
42. There shall be a common interface for all services within a configuration.

## System-Level Properties

1. For every Unique Automation Request, the system shall produce a response (which might be an error message).
2. Every task included in a request message shall be included in the associated response message.
3. If the request and response messages do not have identical task listings, an error shall be produced.
4. The system shall respect airspace constraints
5. Paths produced shall not intersect with a “Keep-Out” zone.
6. Vehicles shall stay in “Keep-In” zones
7. If there is a feasible assignment (mission solution) possible the system shall calculate the solution.
8. If the process algebra relationship is valid (well-formatted), then we shall adhere to the defined relationship.
9. If the process algebra relationship is not valid (not well-formatted), then an error shall be generated
10. Vehicles altitudes shall be distinct and differ by at least X ft
11. Vehicle altitudes shall not be changed during the mission
12. The costs associated with that of tasks and missions shall be influenced by vehicle altitude
13. If a map update is sent by the user, that user will also determine when to force a replan (for the entire system).
14. Assignment cost matrix coming out of route aggregator service shall be defined by the #vehicles\* # task options + # vehicles\* (#task options)^2.
15. Message IDs shall be unique system-wide throughout a mission
16. Route planner shall be configured with vehicle configuration data before a route plan request is sent (or received)?
17. Messages shall be received in the order in which they were sent
18. The system shall propagate error messages to the final recipient
19. ~~For each request sent, a response (possibly an error) is received and that response corresponds to that request.~~
20. A sent request message shall have a corresponding response or error message.

## Proposed Requirements

1. The configuration shall report an error if an automation request is received but the requested resource has not been defined
2. ~~Resources include Tasks, Vehicles and Regions~~
3. The configuration shall generate a UniqueAutomationRequest message if an AutomationRequest is received and the requested resource has been defined
4. The configuration shall publish UniqueAutomationRequest messages in the order in which they are generated
5. The configuration shall publish one UniqueAutomationRequest message and wait for a corresponding UniqueAutomationResponse message to be received
6. The configuration shall publish the next UniqueAutomationRequest message immediately if there is no outstanding UniqueAutomationResponse message
7. Optionally, the configuration shall publish the next UniqueAutomationRequest if the outstanding UniqueAutomationResponse message has not been received within a set time
8. The configuration shall publish an AutomationResponse message in response to the corresponding AutomationRequest message when a corresponding UniqueAutomationResponse message is received
9. The configuration shall ensure that only one AutomationRequest is executed at a time

## RouteAggregator Requirements

1. The configuration shall create a unique RoutePlanRequest message for each vehicle ID in each RouteRequest message received
2. The configuration shall send each RoutePlanRequest message to the planners that are appropriate for the associated vehicle type
3. The configuration shall correlate RoutePlanReponses with RoutePlanRequests
4. The configuration shall send a RouteResponse message when all RoutePlanResponses are received for a particular RouteRequest

## RoutePlannerVisibility Requirements

1. The configuration shall generate a route for each pair of start and end locations specified in each RoutePlanRequest message received
2. Route generation shall be efficient
3. Route generation shall be responsive
4. Routes shall be approximately distance optional
5. Routes shall respect vehicle limitations
6. ~~Vehicle limitations include minimum turn radius constraints~~
7. The configuration shall send a RoutePlanResponse message using return-to-sender addressing when a route has been generated for all pairs of start and end locations specified in the associated RoutePlanRequest message
8. The configuration shall take environment and vehicle constraint information from appropriate inputs

## Secure Communication Requirements

1. UxAS shall ensure communication is only between intended services.
2. UxAS shall ensure data is only accessible to services with proper permission authority.
3. UxAS communication channels shall be always available to intended users.
4. UxAS will filter out garbage data from communication channels.
5. UxAS shall detect the authenticity of incoming messages.
6. UxAS will detect if an attacker resends an old message.
7. UxAS will encrypt communications.
8. UxAS shall verify received messages are from a source authorized to send the given message type.