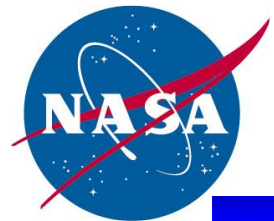


Resilient Autonomy in the Face of Adversity

Ethan Williams

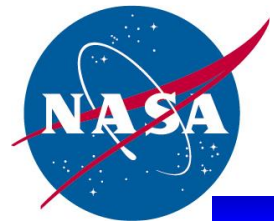
Resilient Autonomy Project Software Lead



Abstract



- The NASA Resilient Autonomy Project developed a software framework that implemented a Run Time Assurance (RTA) architecture that leveraged ASTM International's F3269 Industry Standard for safely bounding complex behavior in aircraft. This framework was called the Expandable Variable Autonomy Architecture, or EVAA. EVAA was developed during the height of the Covid-19 lockdown that caused the Resilient Autonomy team to pivot from flight test to distributed simulator testing. EVAA was developed to be platform and mission agnostic where platform specifics were behind a hardware abstraction layer that EVAA called a Coupler. EVAA was able to host multiple safety monitors that could resolve individual safety hazards. EVAA was able to resolve priority conflicts when multiple safety hazards needed to be resolved simultaneously and was able to resolve highly complex situations in a safe manner that could exceed human capabilities.



Resilient Autonomy

Technology & Airworthiness Development & Transition



Performance Based Certification

F-16 Auto GCAS & ACAS



USAF
F-16 & F-35

AvSP



ASTM
International

1st Industry Standard



UTM & SASO



2018 Collier

Resilient Autonomy

Joint Capability Technology Demonstration



Reference Implementation Development

NASA

UAM

Autonomy
Safety
Standards

Industry

Drone
Package
Delivery

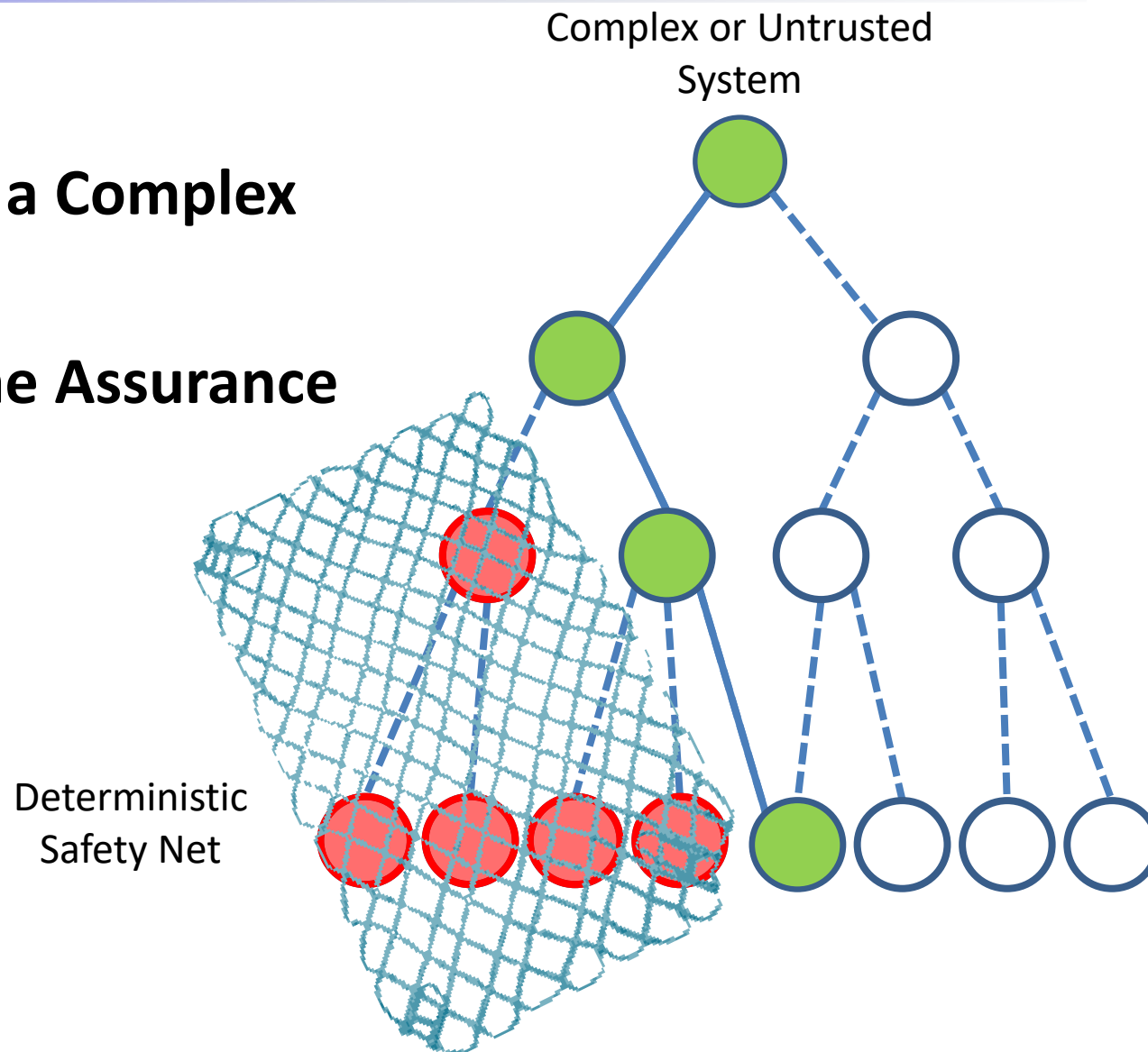
DoD

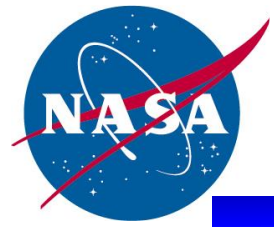
Army
Future
Vertical-Lift &
UAS

USAF
Future Attack
UAS

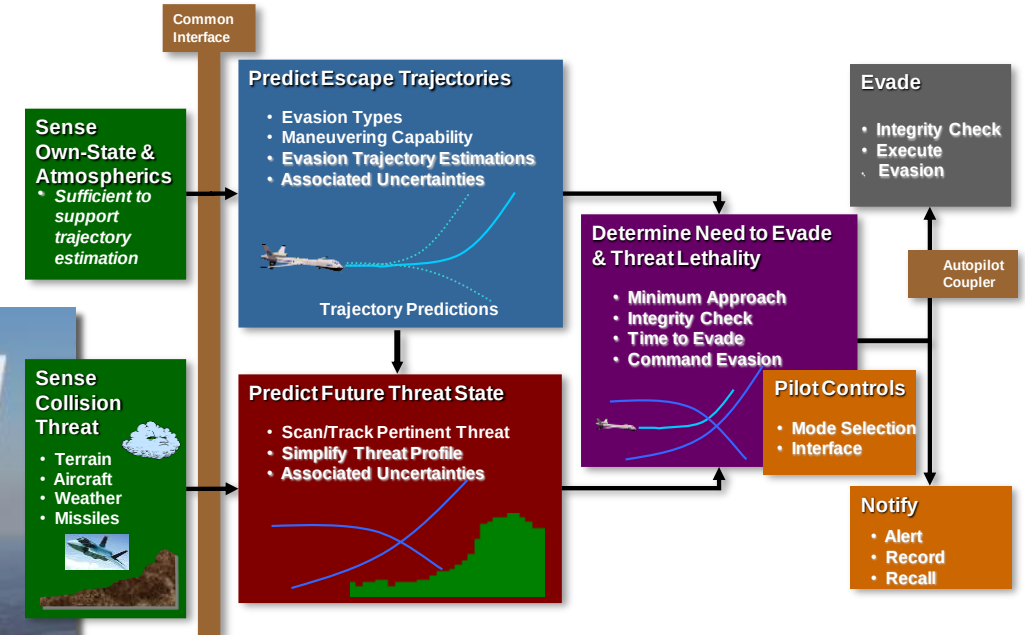
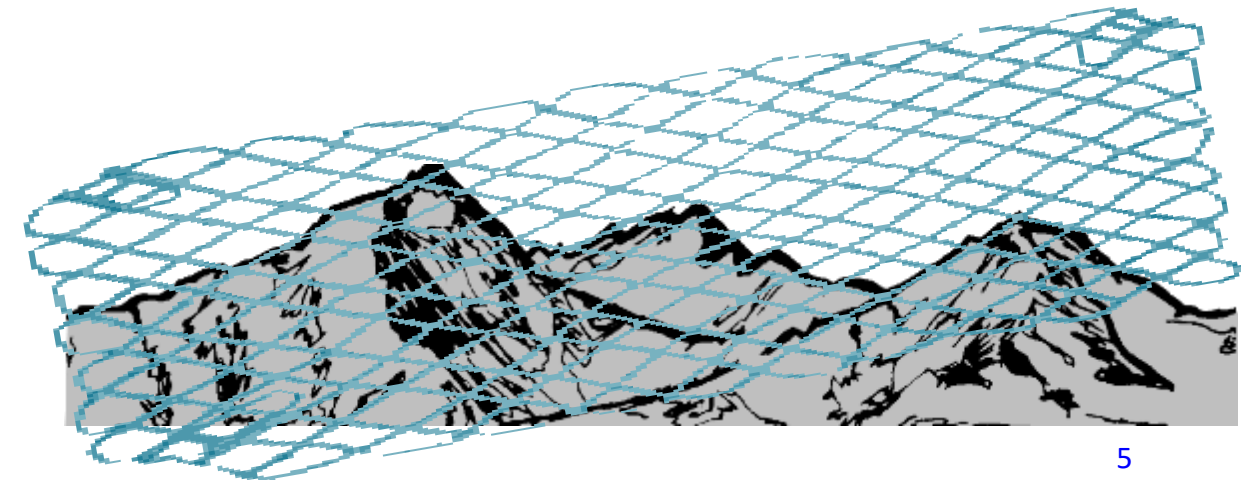
The Challenge of Autonomy

- **Verification & Certification of a Complex System**
- **A Possible Solution – Run-Time Assurance (RTA)**





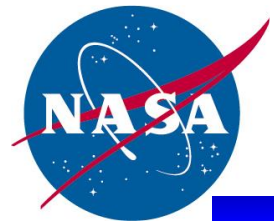
Ground Collision Avoidance System (GCAS)



UNCLASSIFIED



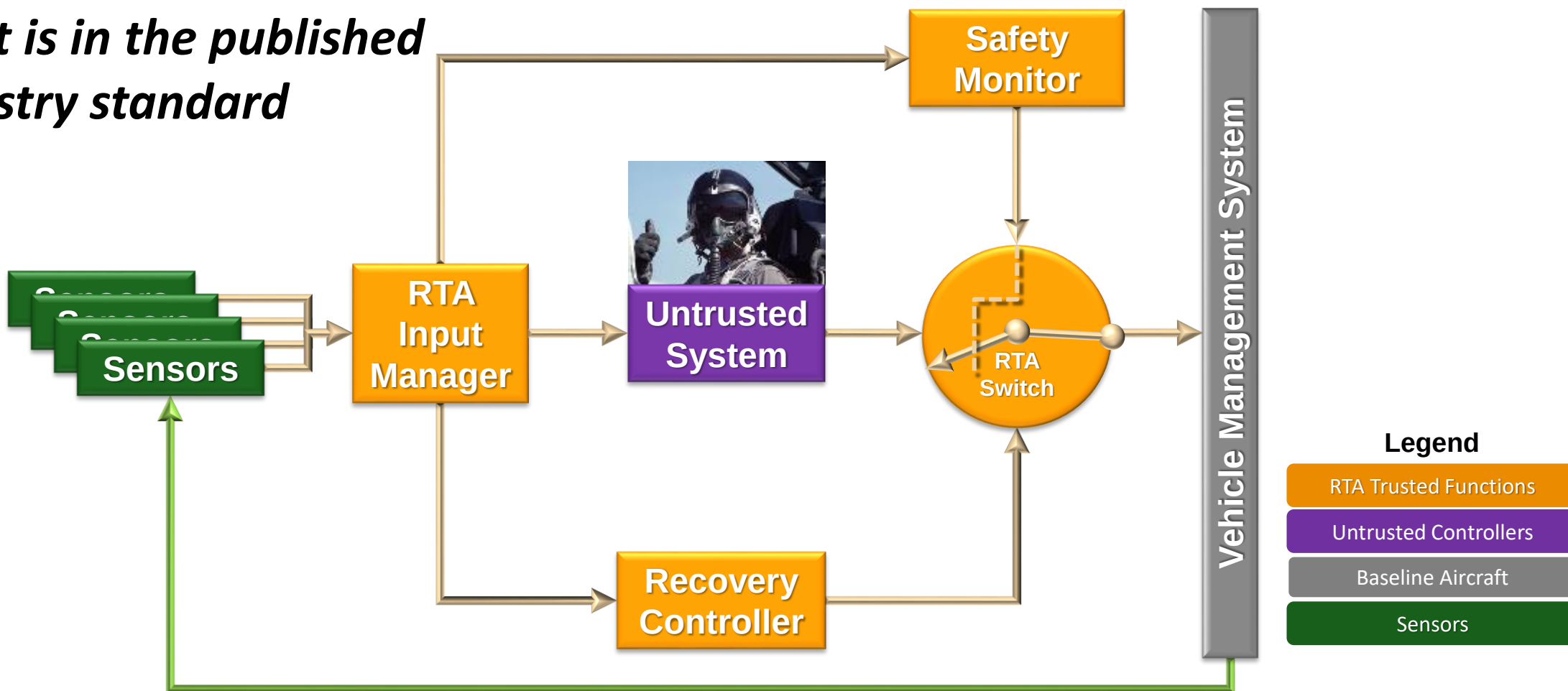
UNCLASSIFIED

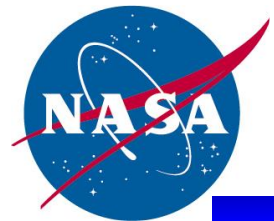


Traditional RTA Framework



This illustration represents what is in the published industry standard



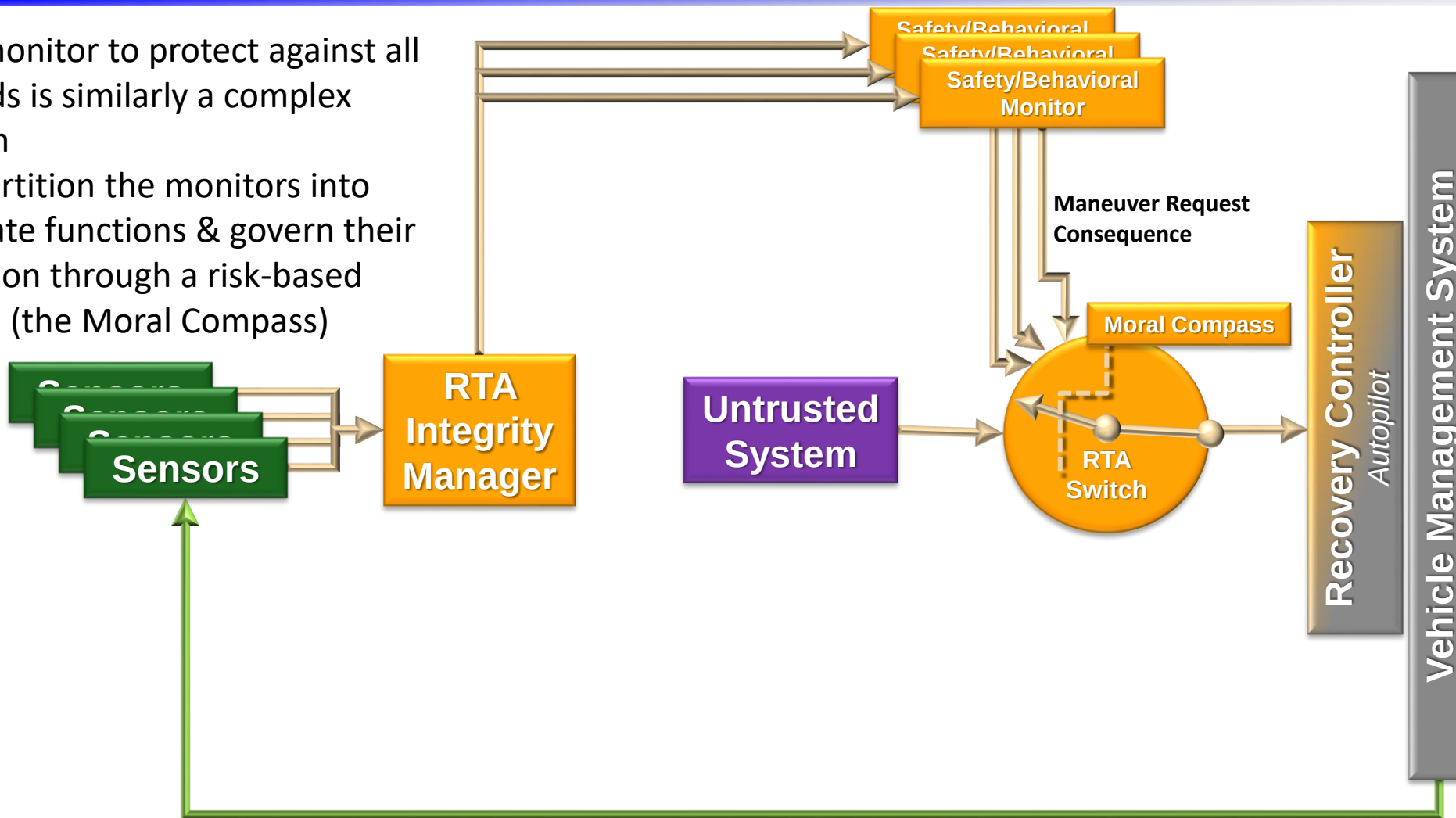


MM-RTA Framework



EVAA Phase 1 : 2017

- One monitor to protect against all hazards is similarly a complex system
- We partition the monitors into separate functions & govern their selection through a risk-based switch (the Moral Compass)



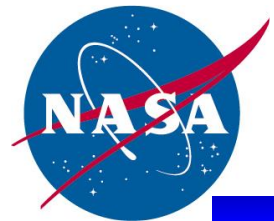
Legend

RTA Trusted Functions

Untrusted Controllers

Baseline Aircraft

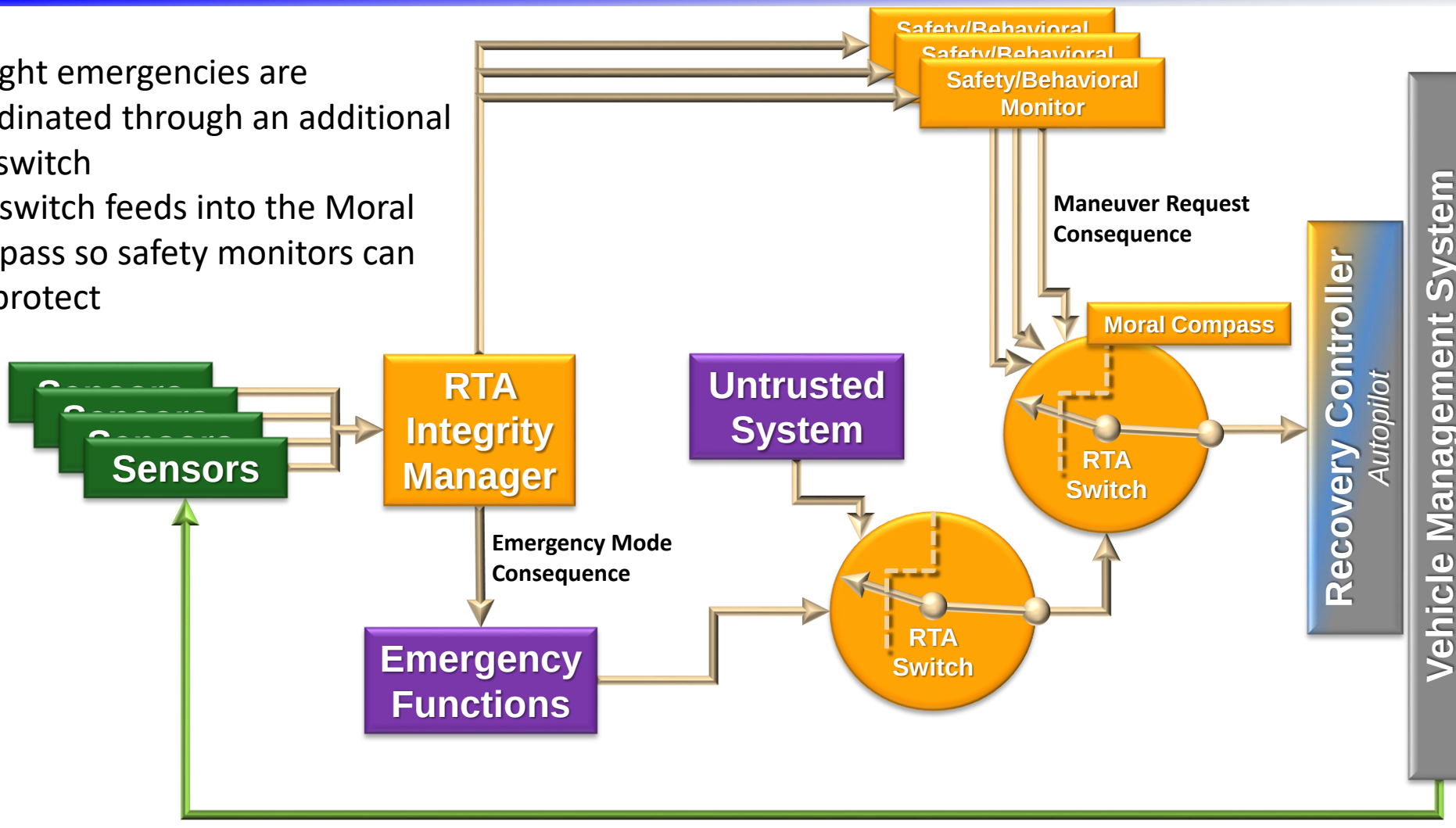
Sensors



Expandable Variable Autonomy Architecture EVAA



- In-flight emergencies are coordinated through an additional RTA switch
- This switch feeds into the Moral Compass so safety monitors can still protect



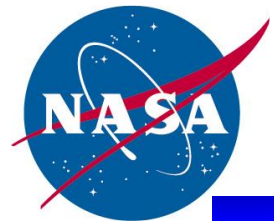
Legend

RTA Trusted Functions

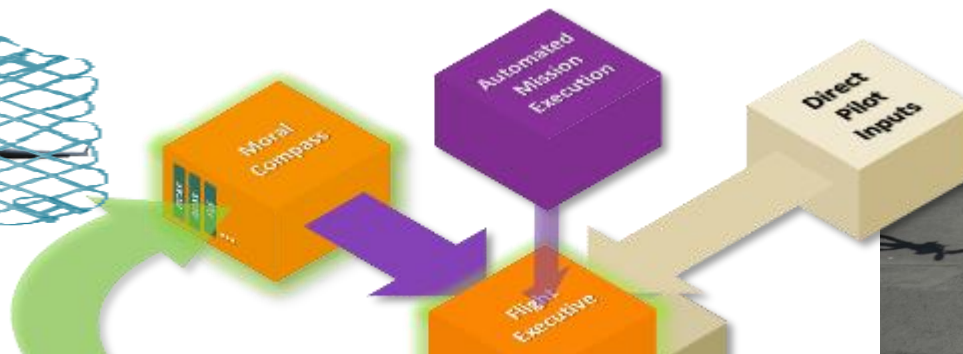
Untrusted Controllers

Baseline Aircraft

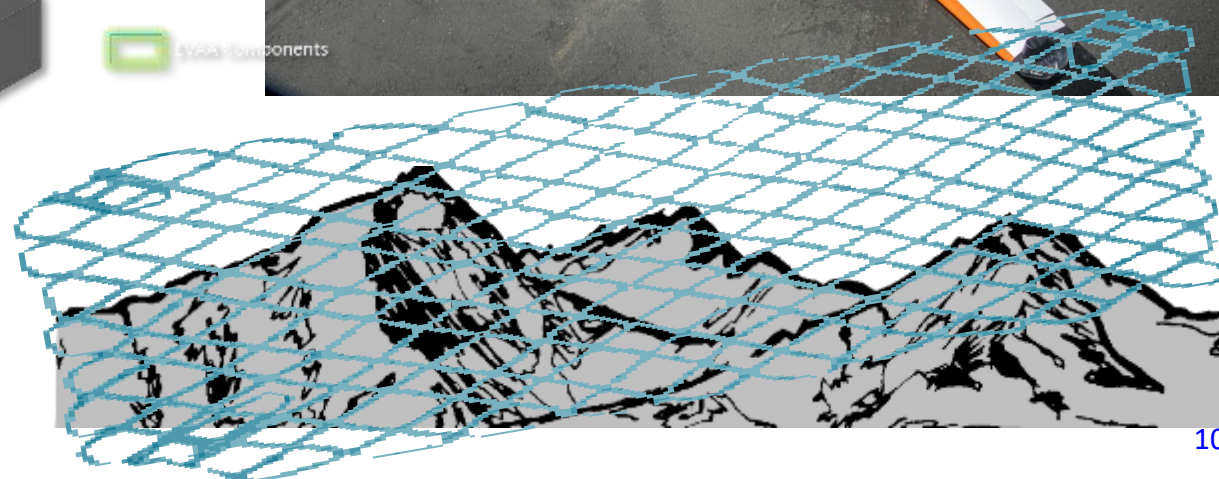
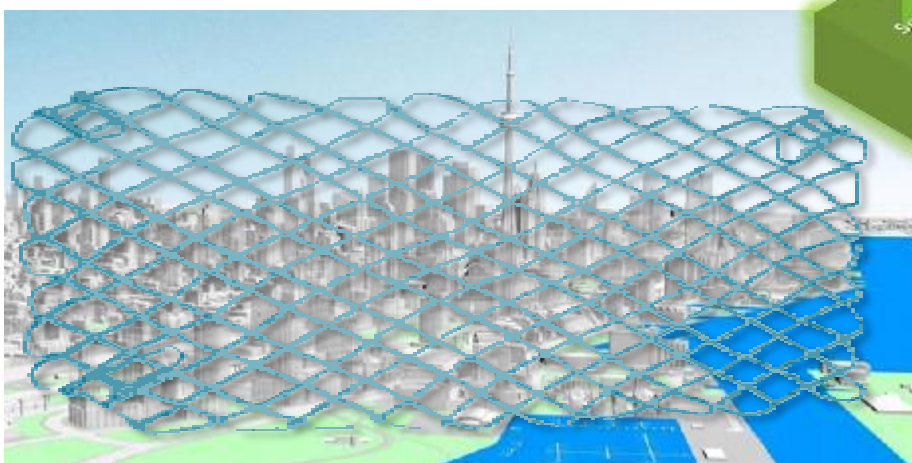
Sensors

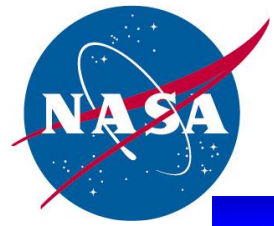


Multi-Monitor RTA (MM-RTA)

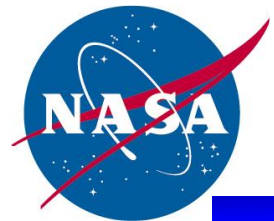


EVA Expandable Variable-Autonomy Architecture





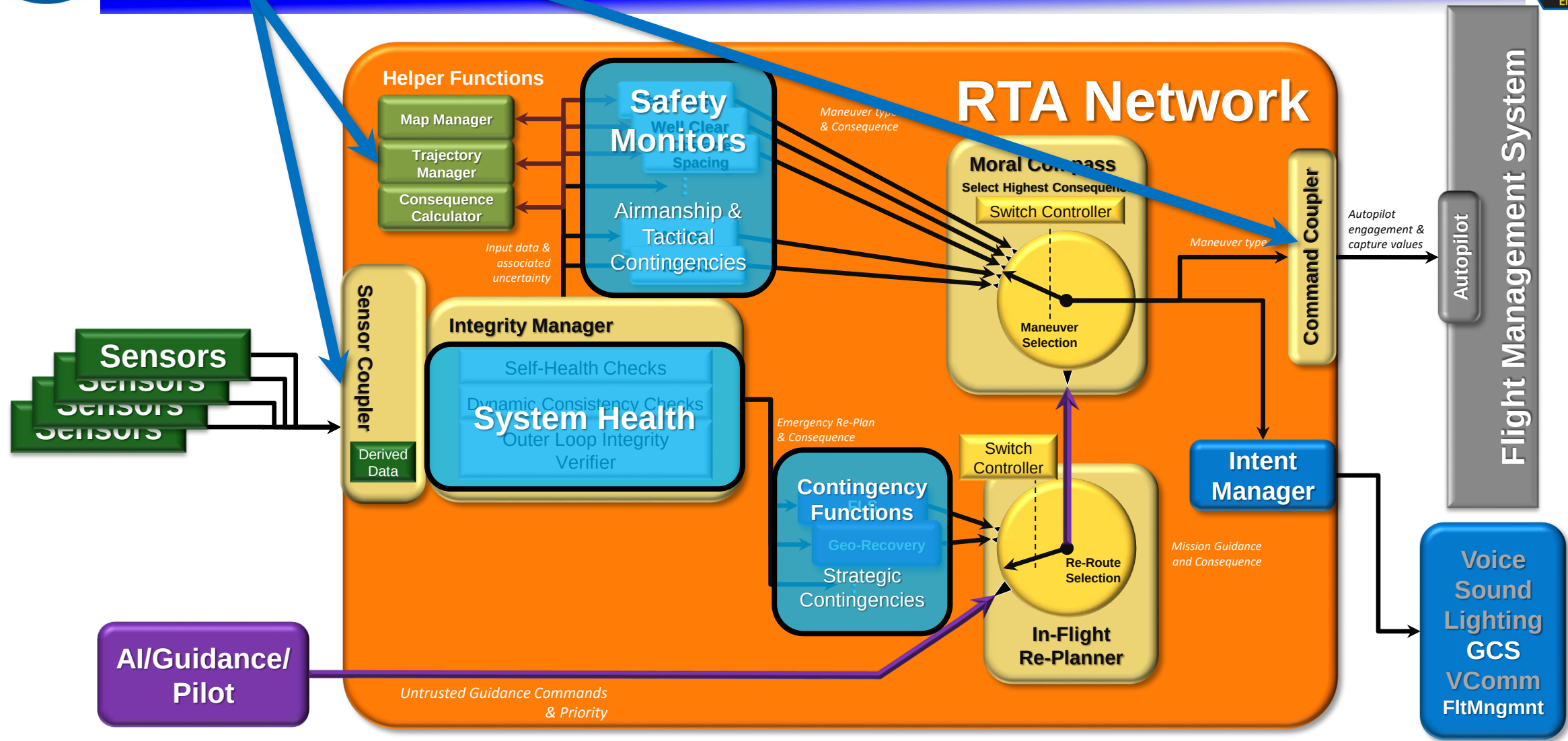
RESILIENT AUTONOMY

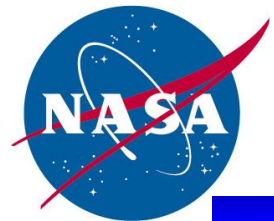


RA JCTD Proposal



- **What is the need?**
 - Effectively & affordably counter threat networks (CTN)
 - *Extend current capability which is limited to 35nm & 5k for Due Regard*
- **What is it?**
 - **Airworthy, Safe, Scalable Autonomy Framework for an Airborne Agent that can react to unanticipated events and situations**
- **What will the project do?**
 - 1. Develop a Government Owned System that can be Adapted to any Vehicle** and allow Link-less & Multi-Aircraft to One Operator Capability DoD-wide
 - 2. Develop and Evaluate an Airworthy System for the HQ-90** UAS that will allow beyond line-of-sight (BLOS) operations in Domestic and International Airspace





The HQ-90/EVAA Reference Implementation



Cooperative Targets

Air Traffic Detection



SARA Acoustic



ADS-B



Echodyne
Radar



Navigation



GPS

INS

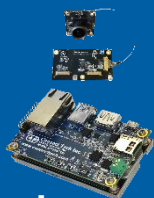
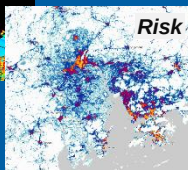
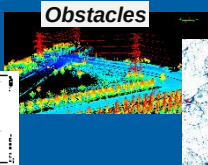
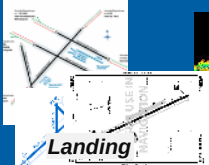


Image
Referenced
Navigation



Visual Inertial
Odometry

Ground/Obstacle/Risk Detection



Digital Maps

Aircraft Control



EVAA Autonomy

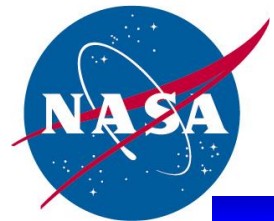


Autopilot

Aircraft



- 117 Lbs. Max Gross Takeoff Weight
- 14' 8" Wingspan
- 11 pounds of Payload
- Up to 15 Hours Endurance

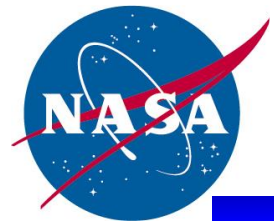


Initial Proposal



- Implement it on an L3-Harris HQ90
- Centralized Simulator



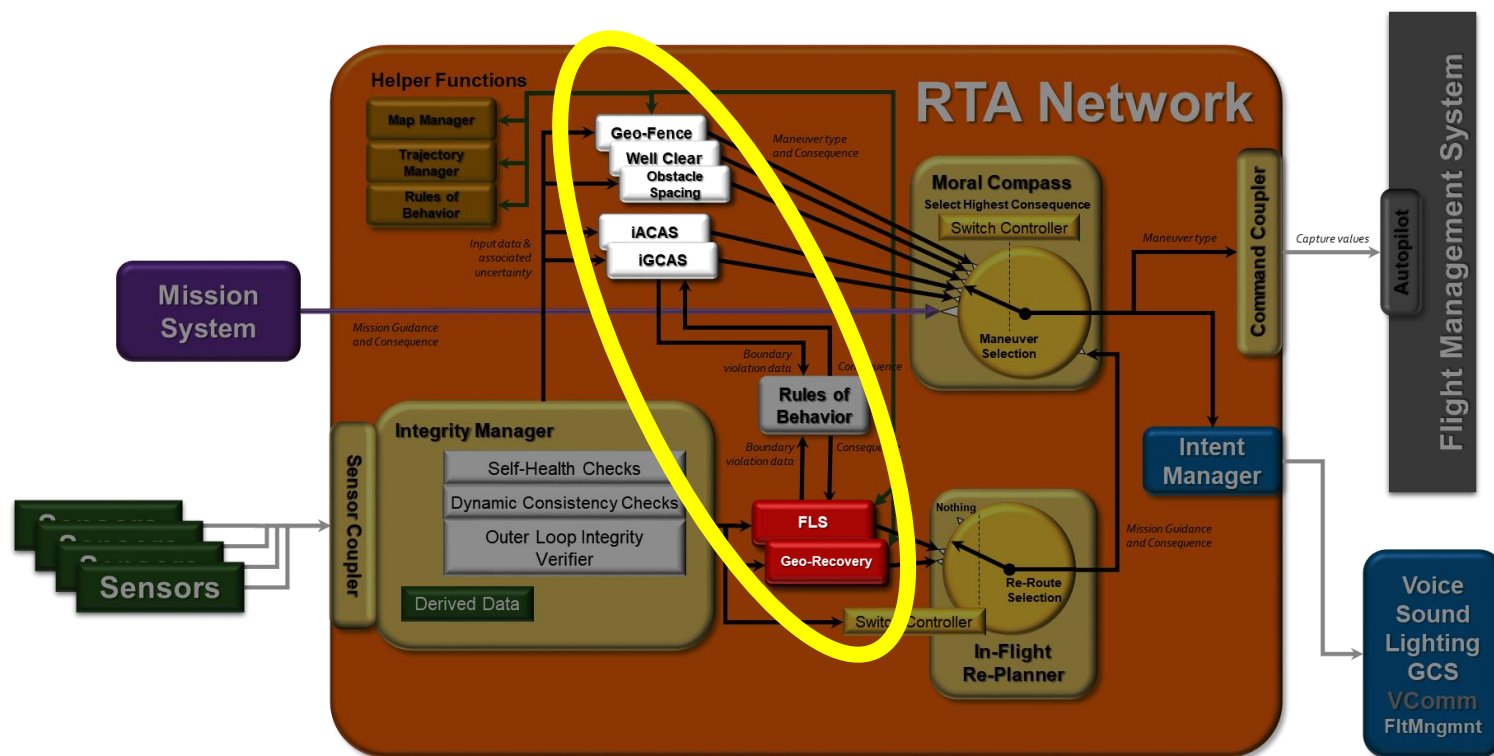


Global Lockdown



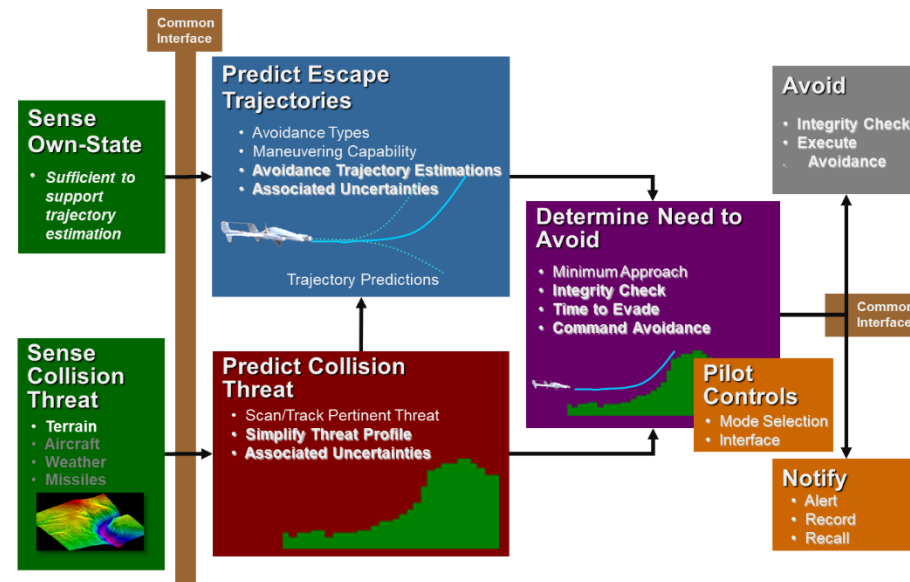
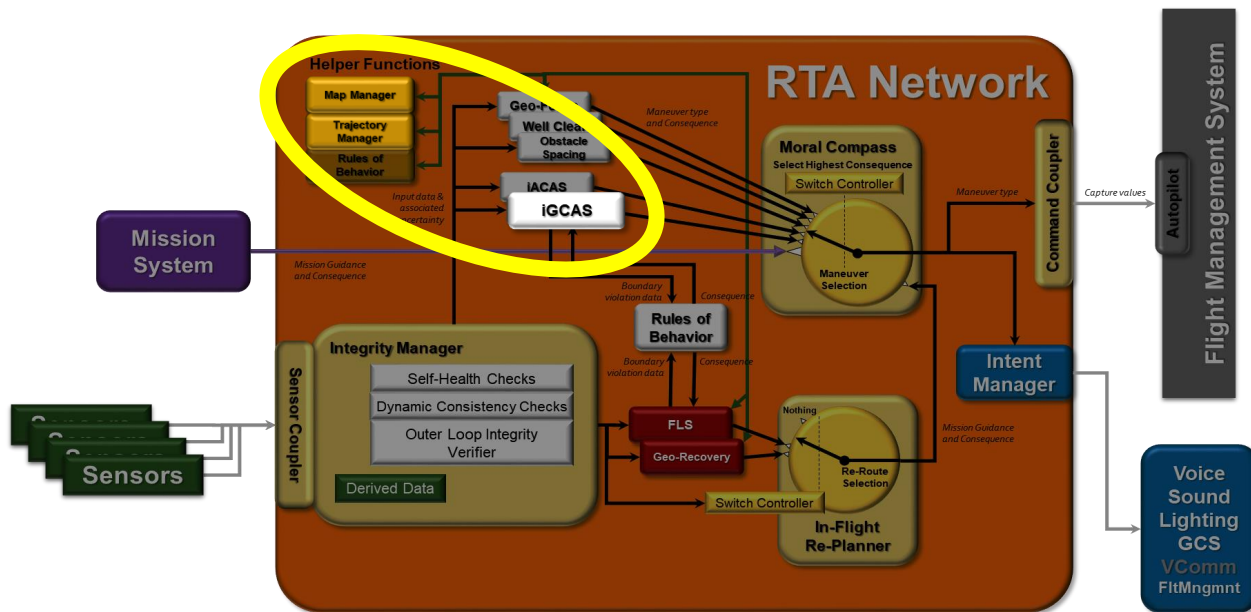
- Occurred just before flight test
- Indefinite stop to flight test
- Quickly distributed simulator components to team
- Remainder of the RA project conducted via remote distributed simulations
- Utilized MS Teams as a remote control room





Monitors & Emergency Re-planners

THE ALGORITHMS



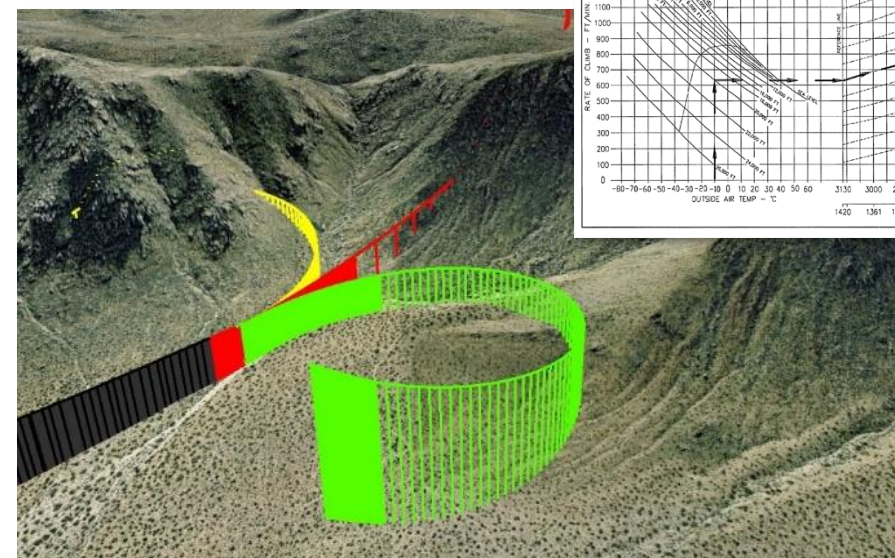
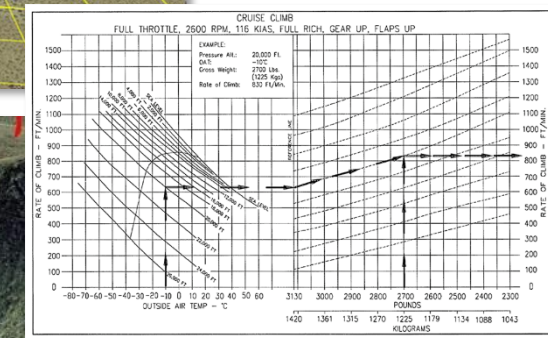
IGCAS

Improved Ground Collision Avoidance System

- Trajectory Manager
- Map Manager

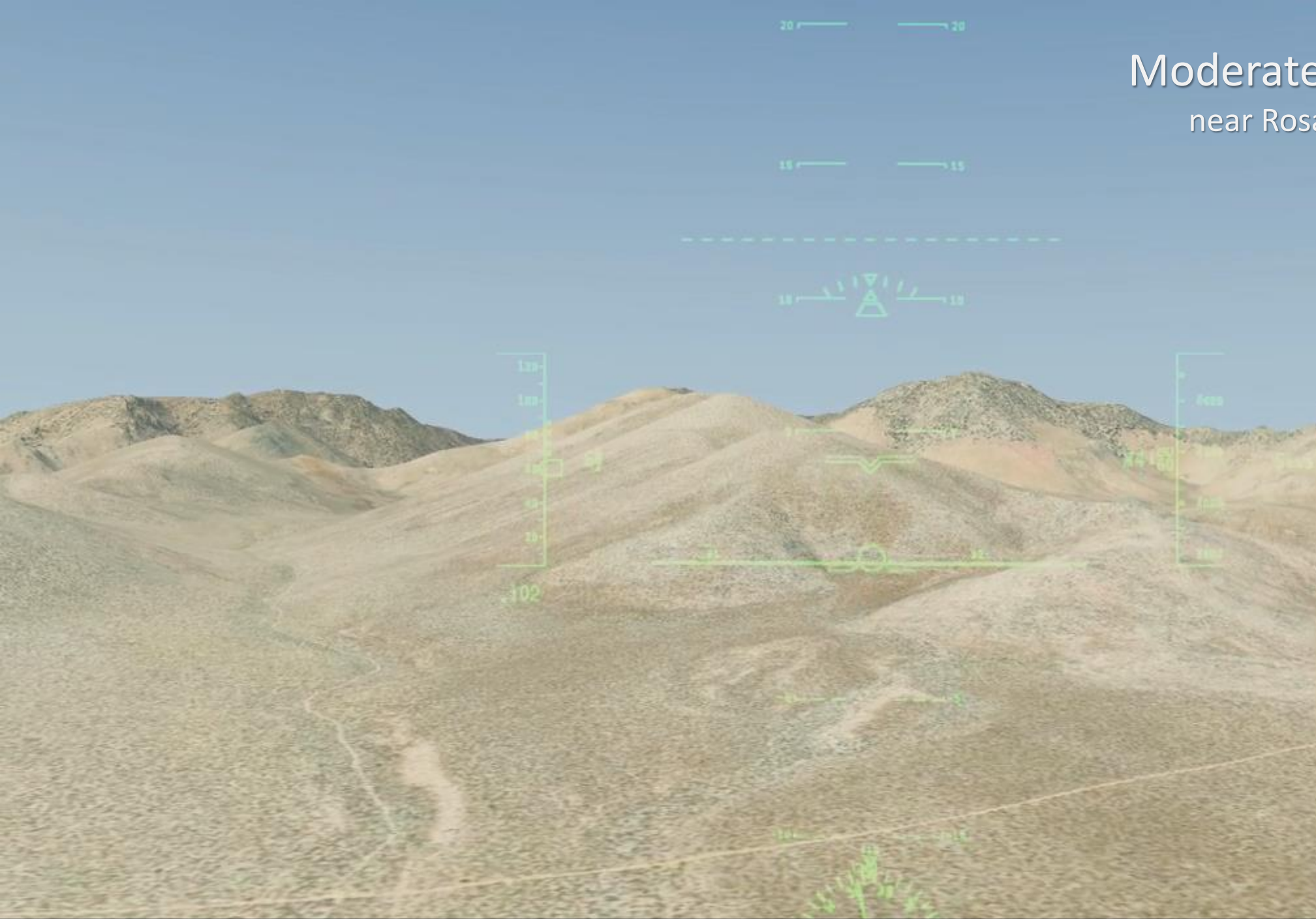


-



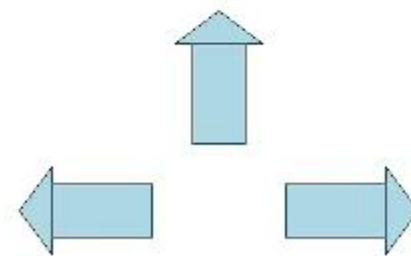
Moderate Terrain

near Rosamond

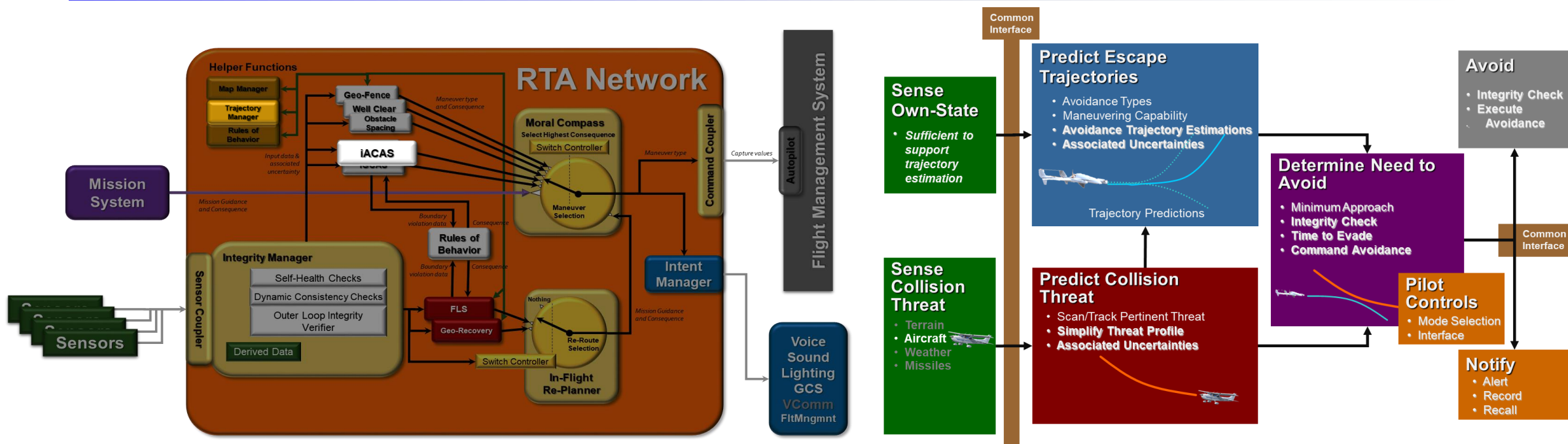


Pilot

Manual Flight



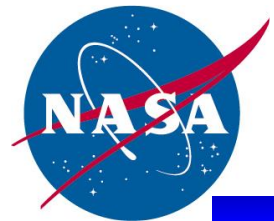
999.00 46.07 999.00



IACAS

Improved Air Collision Avoidance System

- Trajectory Manager



iACAS Design



- **Purpose**

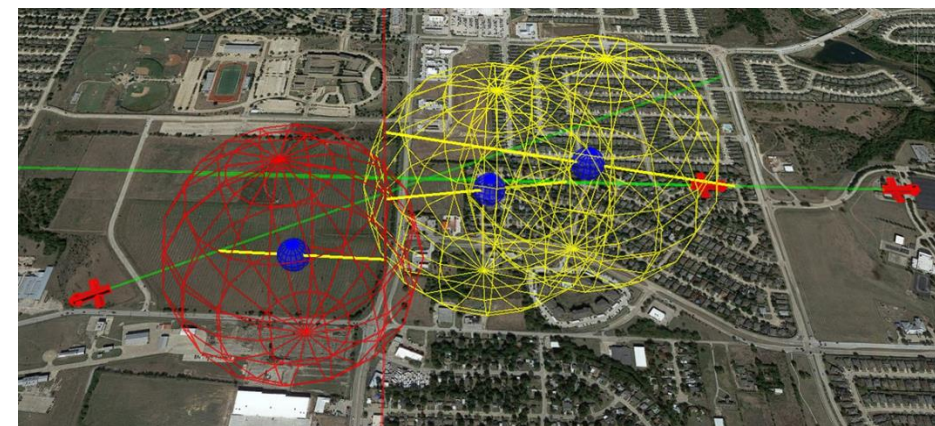
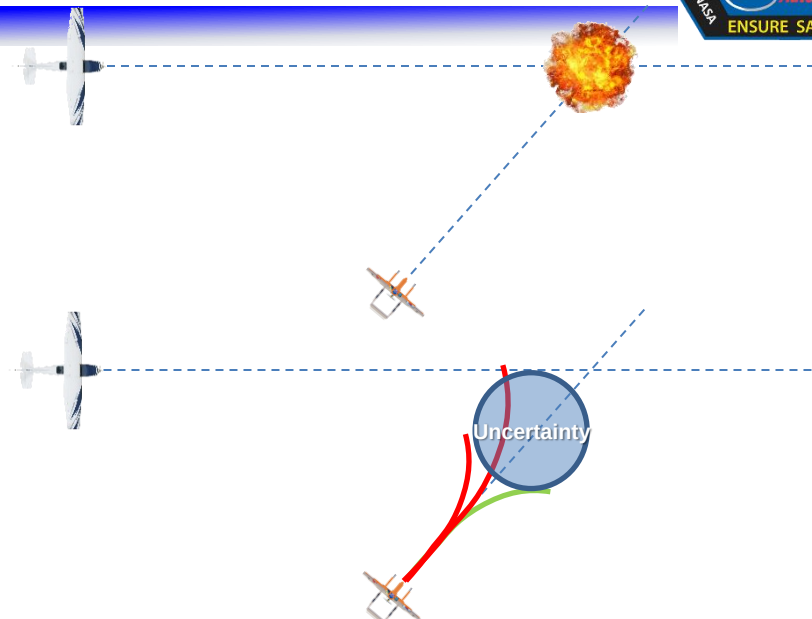
- Avoid midair collisions and request an aggressive escape maneuver

- **Basic Concepts**

- Generates multiple Escape Trajectory Options
- Evaluates Separation of Each
- Waits Until Last Maneuver can Barely Avoid to Request that Maneuver

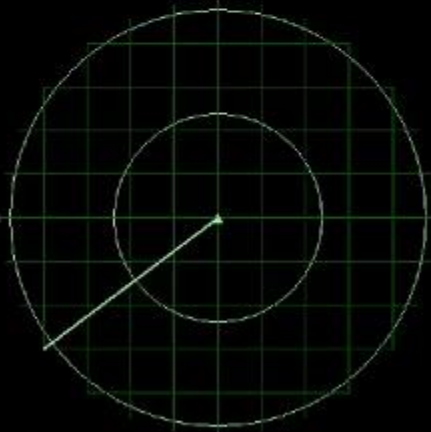
- **Capability**

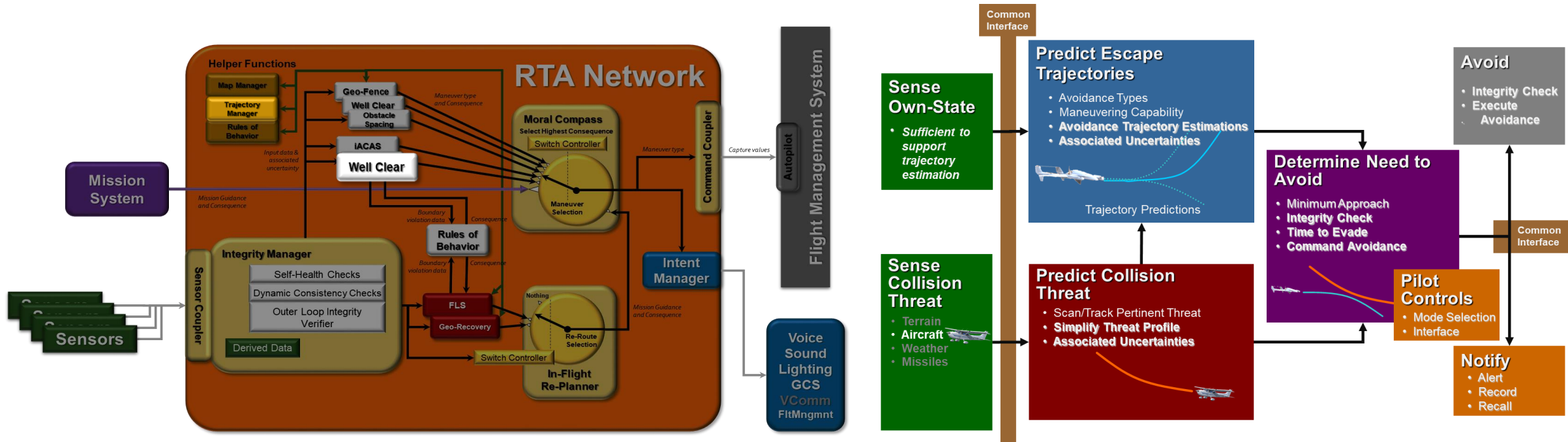
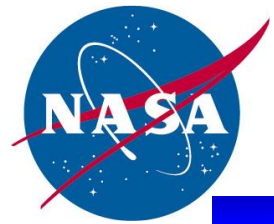
- Any Number of Intruder Aircraft
- Any Type and Number of Avoidance Options
 - Currently using 7 avoidance options
 - Maneuvers are aggressive & like those used by iGCAS
 - Maneuver profiles are generated by the Trajectory Manager
- Easily Tailors to Aircraft Dynamics
- Additional DAA Sensors Easily Added
 - ADS-B
 - Echodyne Radar 1 to 2 km (only detects aircraft @ $\pm 60^\circ$ Az)
 - Sara Acoustic Sensor 2 to 10 km (only detects propeller aircraft to include helicopters)



Pilot

Manual Flight

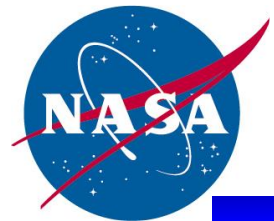




WELL CLEAR

Observing Airmanship Rules

- Trajectory Manager



Well Clear Design



- **Purpose**

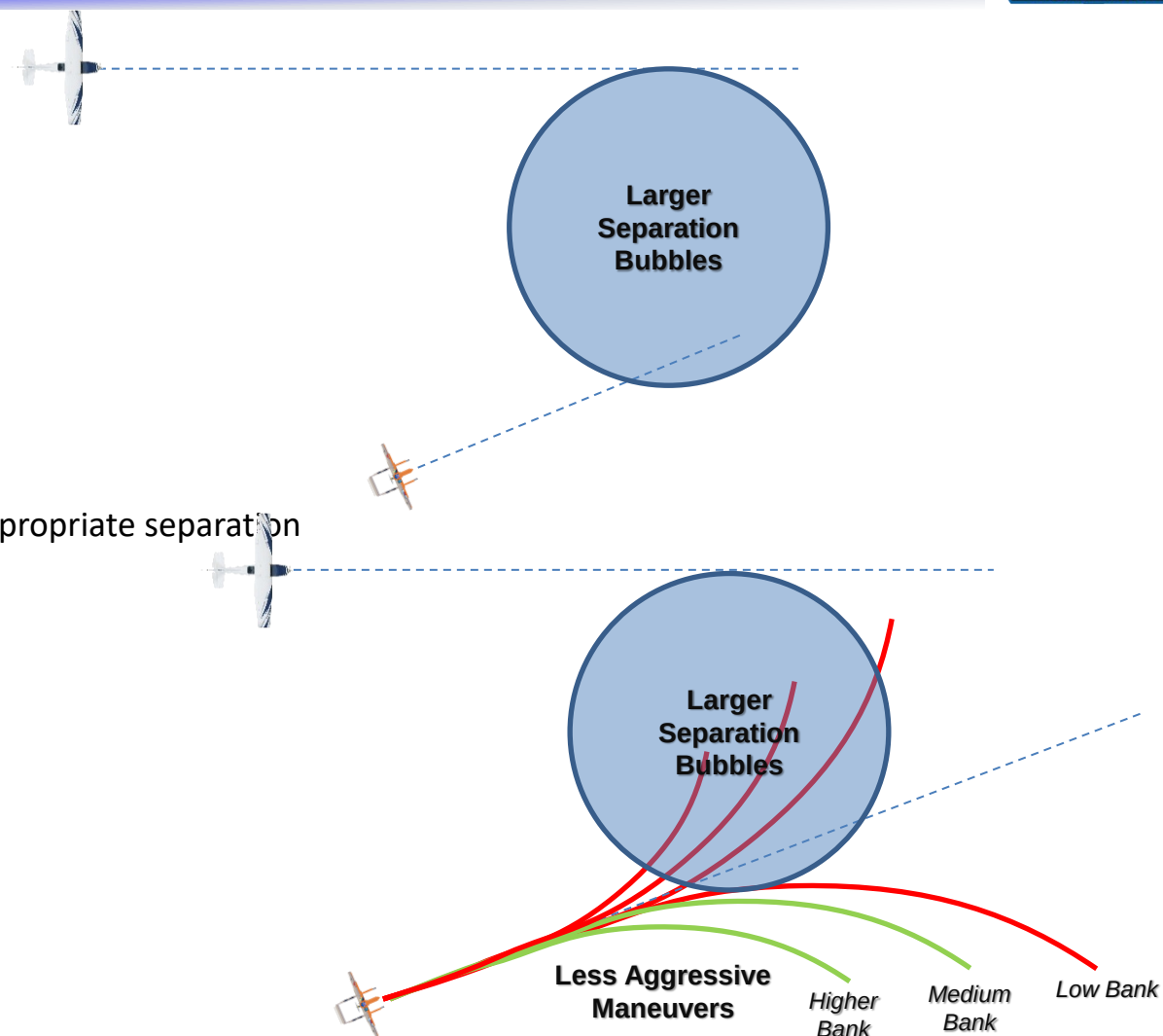
- Observe appropriate airmanship behavior

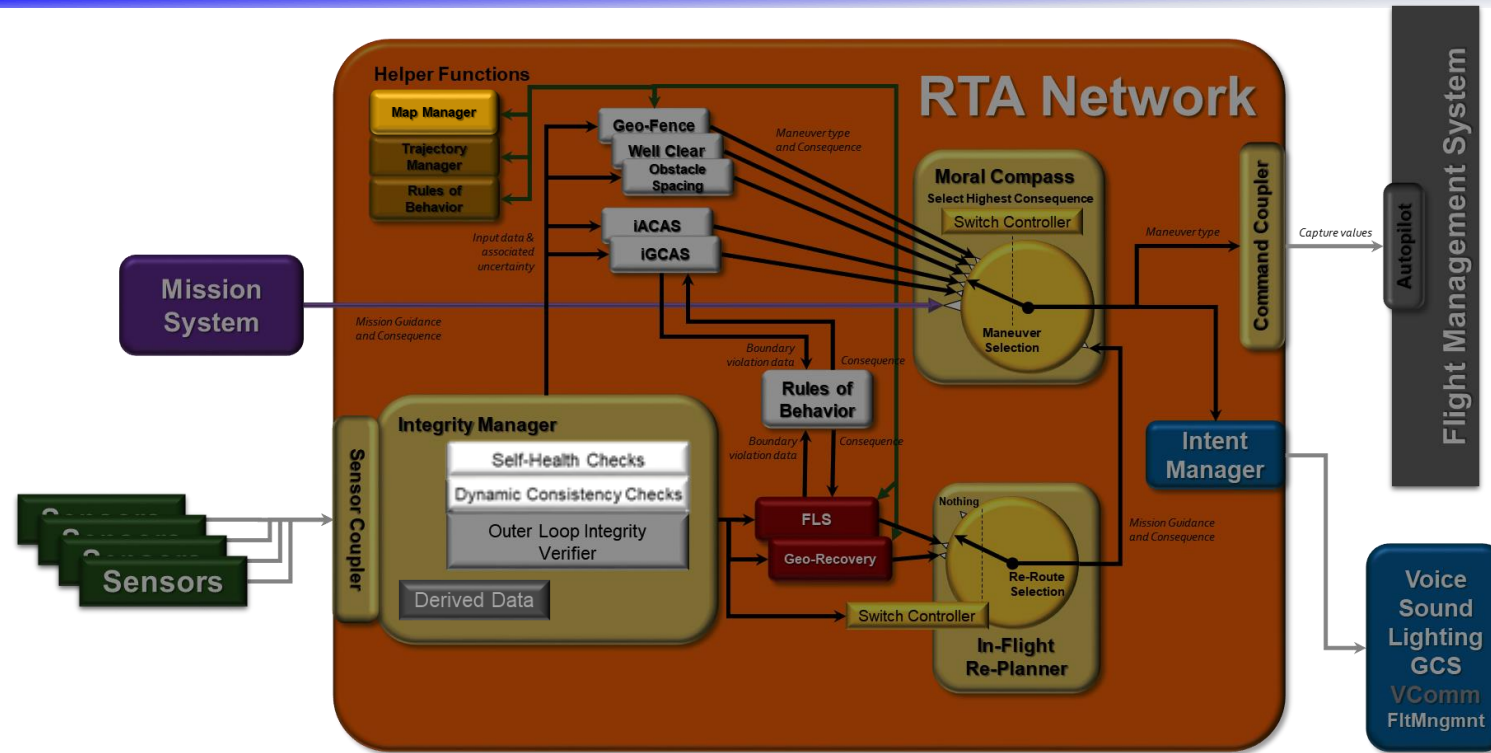
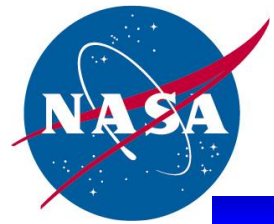
- **Basic Concepts**

- Detune iACAS
 - Larger separation
 - Less aggressive maneuvers
 - Less bank angle used
 - Will increase bank angle used if still not maintaining appropriate separation
 - Dive to “shielded” airspace

- **Capability**

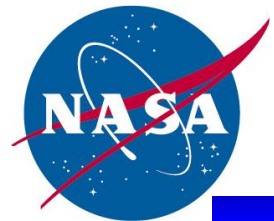
- Acts before iACAS if intruder is sensed early enough





INTEGRITY MANAGER

- Self-Health Checks
- Dynamic Consistency Checks

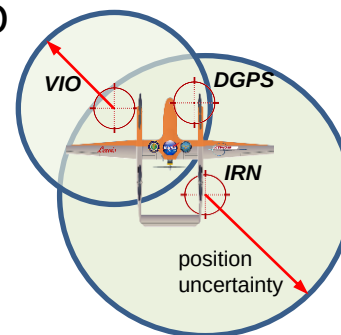


Integrity Manager

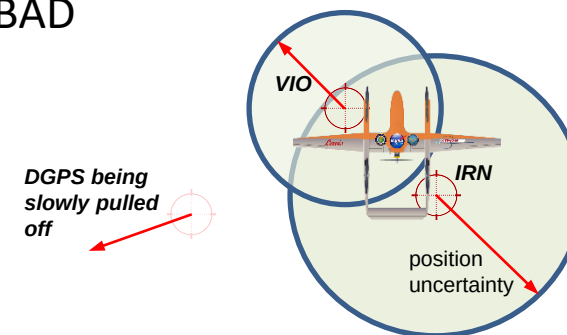


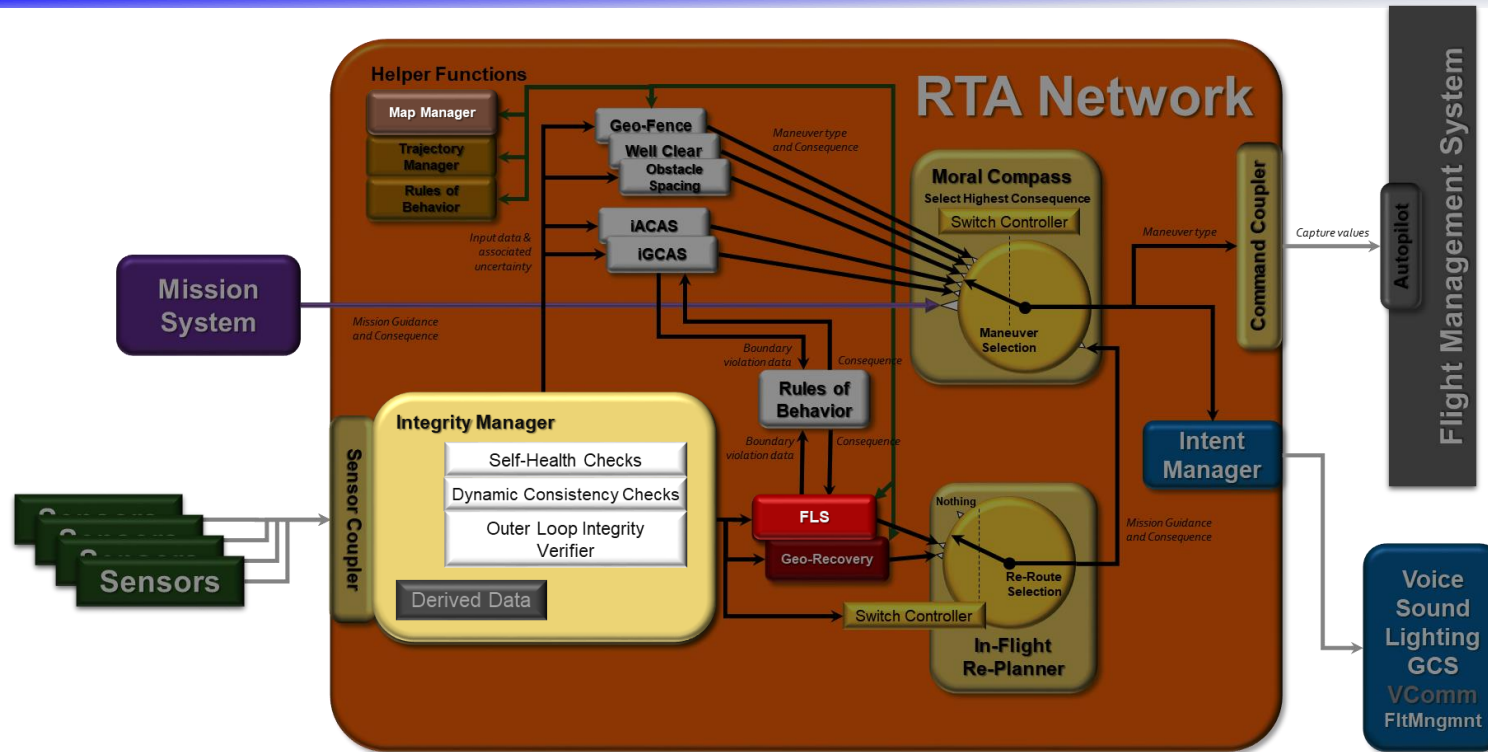
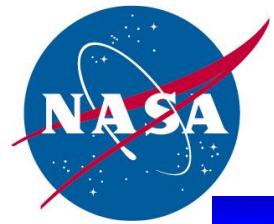
- Each parameter can have its validity checked
 - Self Health Checks (Boundary, Staleness or Delta)
 - Dynamic Consistency Checks (Defined through Plugins)
- Checks are added through human readable configuration files

GOOD



BAD

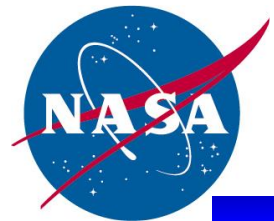




FLS

Forced Landing System

- Integrity Manager
- Map Manager



FLS Design



- **Purpose**

- Generate a flight plan for an emergency landing when contingencies arise that compromise safely continuing the remaining mission

- **Basic Concepts**

- Integrity Management

- Identifies the need for an emergency landing
- Identifies constraints for and how soon the aircraft must land

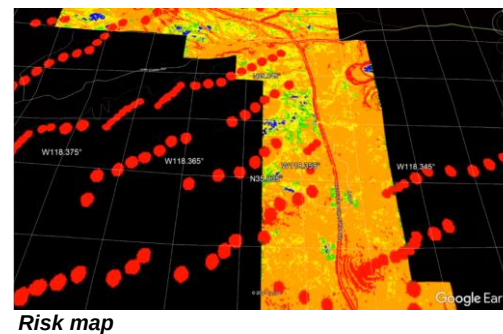
- FLS

- Computes the reachable landing areas
- Requests risk data from the **Map Manager**
 - Provides the lowest risk location for each reachable area
- Sends the landing location to the flight control system and requests landing initiation

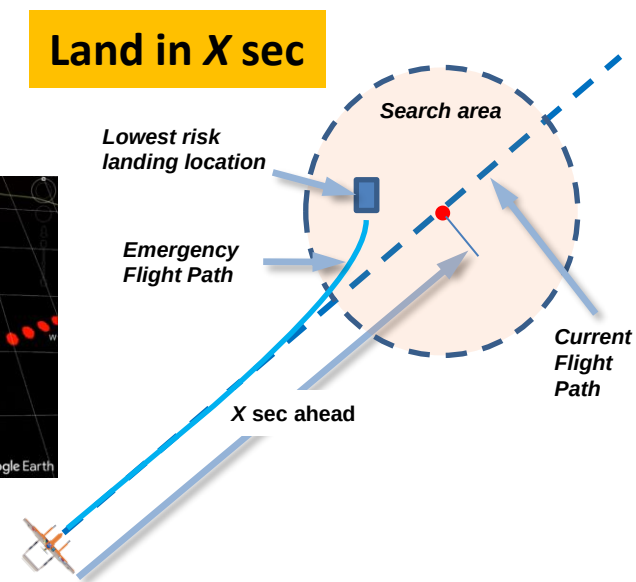
- **Capability**

- Risk map allows significant flexibility

- Currently configured to generate landing risk from LiDAR data
 - Terrain slope & small obstructions
 - Road/highway data from available vector maps
 - Population data

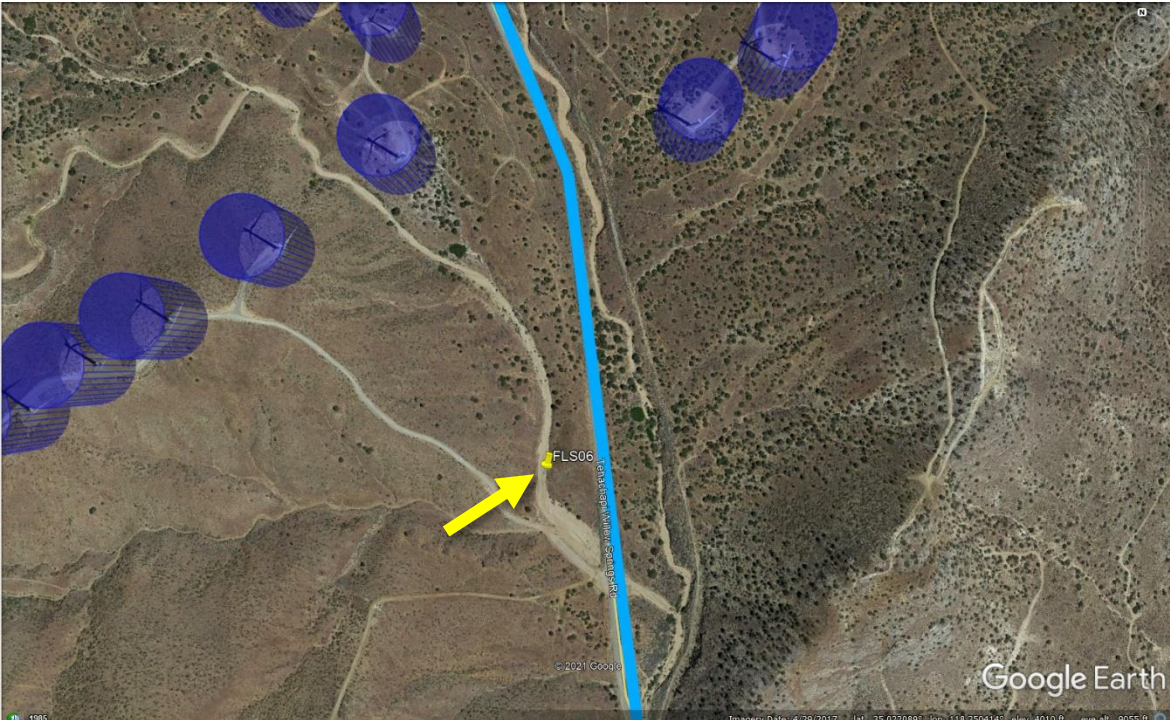


Risk map



• Landing Location

- Picture taken pointing south
 - Orange circle at the landing location
 - Cones were placed at an 8' radius
- Area
Rugged Terrain Windmill Farm
- Landing Location Evaluation
 - Small gully road
 - The only acceptable landing location in the entire area



GPS Anomaly Forced Landing

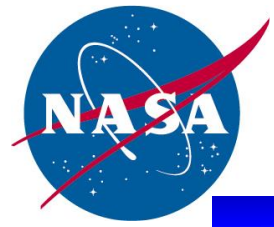


PF

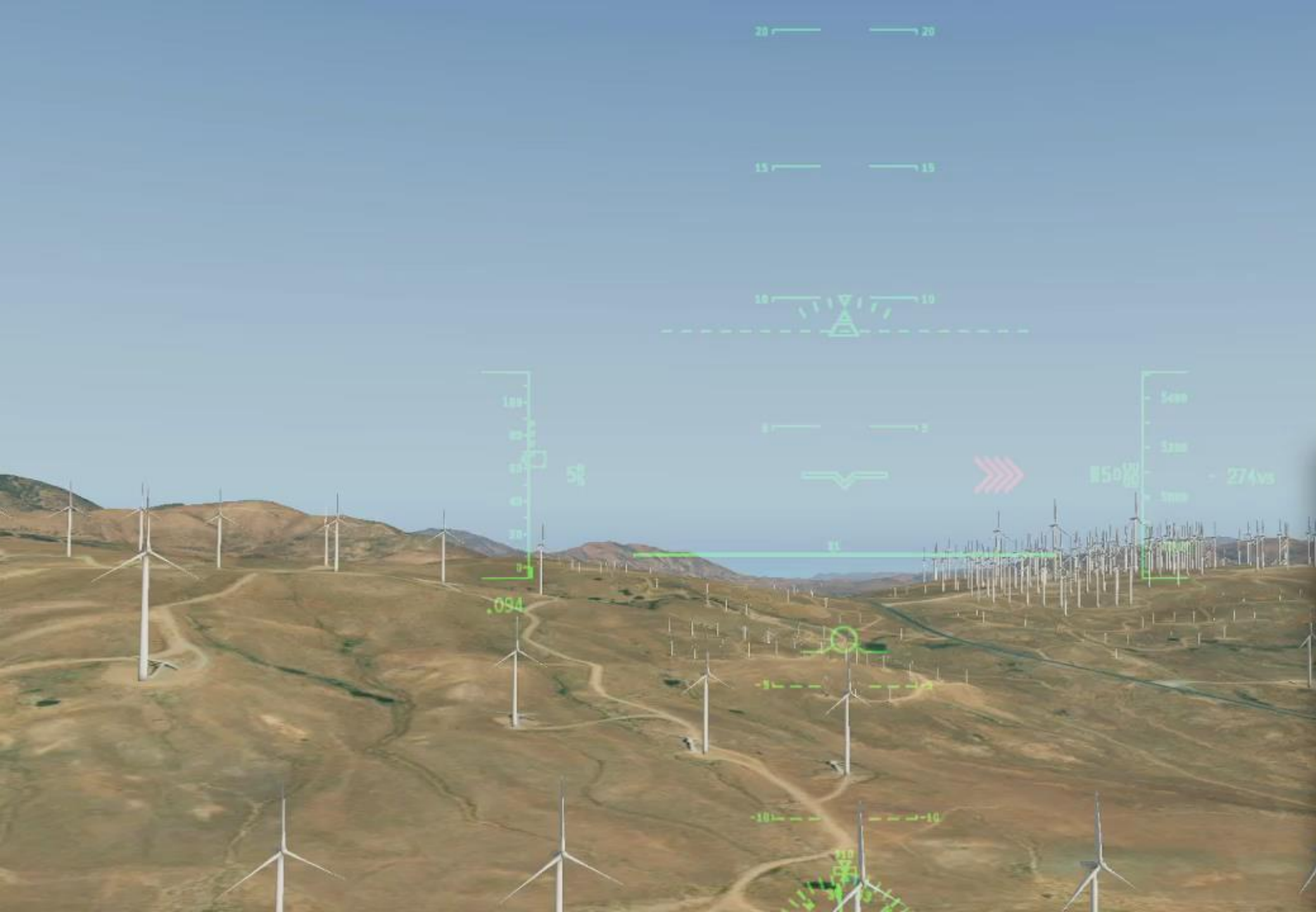
Terrain Following

GPS: Good

Using: GPS



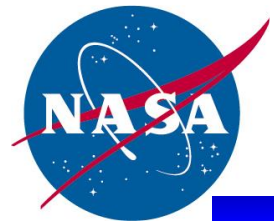
REACTION TO UNPLANNED EVENTS



Well Clear

Dive

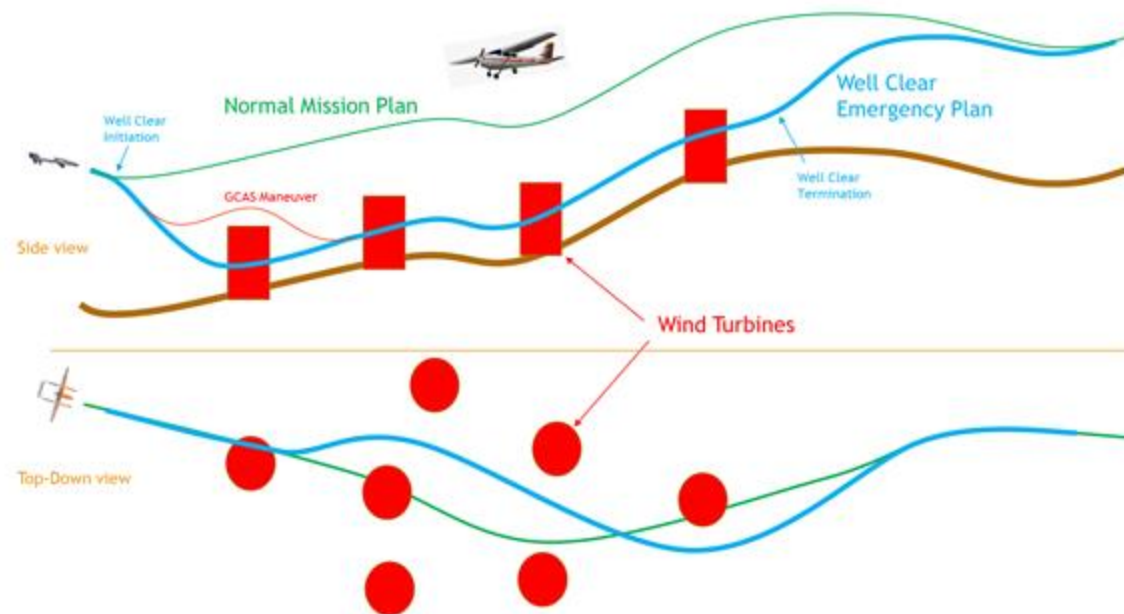


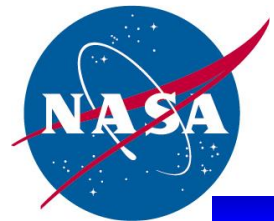


Complex Unplanned Events



- Identify the highest threat at any given instant
- Spread complex situation into individual hazards
- Resolve each hazard in sequence





Resilient Autonomy Conclusions



- EVAAs ability to resolve Complex Unplanned Events exceeds human performance
- The EVAA Multi-Monitor RTA architecture, or similar, should be considered for use on all autonomous vehicles