https://ntrs.nasa.gov/search.jsp?R=20190027053 2019-09-26T19:07:40+00:00Z

SWS High-Level Overview
June 20, 2019

John Koelling, Project Manager

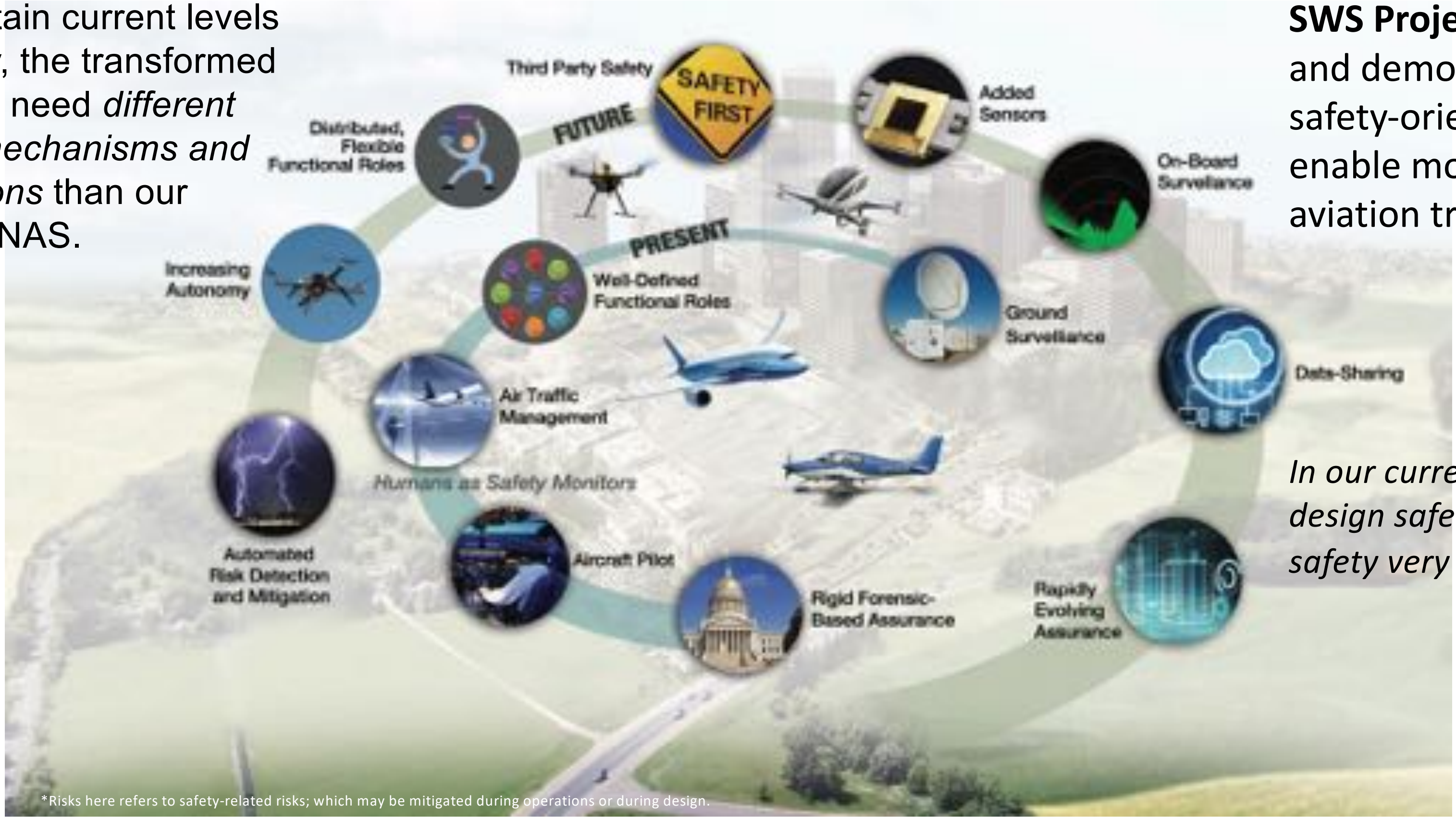
Dr. Misty Davies, Deputy Project Manager

Dr. Kyle Ellis, Associate Project Manager

System Wide Safety

Executive Summary
Top Down Strategy – Airspace Safety

To maintain current levels of safety, the transformed NAS will need *different safety mechanisms and protections* than our present NAS.


Third Party Safety
SAFETY FIRST
FUTURE
Added Sensors
On-Board Surveillance
Distributed, Flexible Functional Roles
PRESENT
Well-Defined Functional Roles
Increasing Autonomy
Ground Surveillance
Data-Sharing
Air Traffic Management
Humans as Safety Monitors
Automated Risk Detection and Mitigation
Aircraft Pilot
Rigid Forensic-Based Assurance
Rapidly Evolving Assurance

*Risks here refers to safety-related risks; which may be mitigated during operations or during design.

SWS Project Goal: To develop and demonstrate innovative safety-oriented solutions that enable modernization and aviation transformation.

In our current system, we treat design safety and operational safety very differently.

System Wide Safety

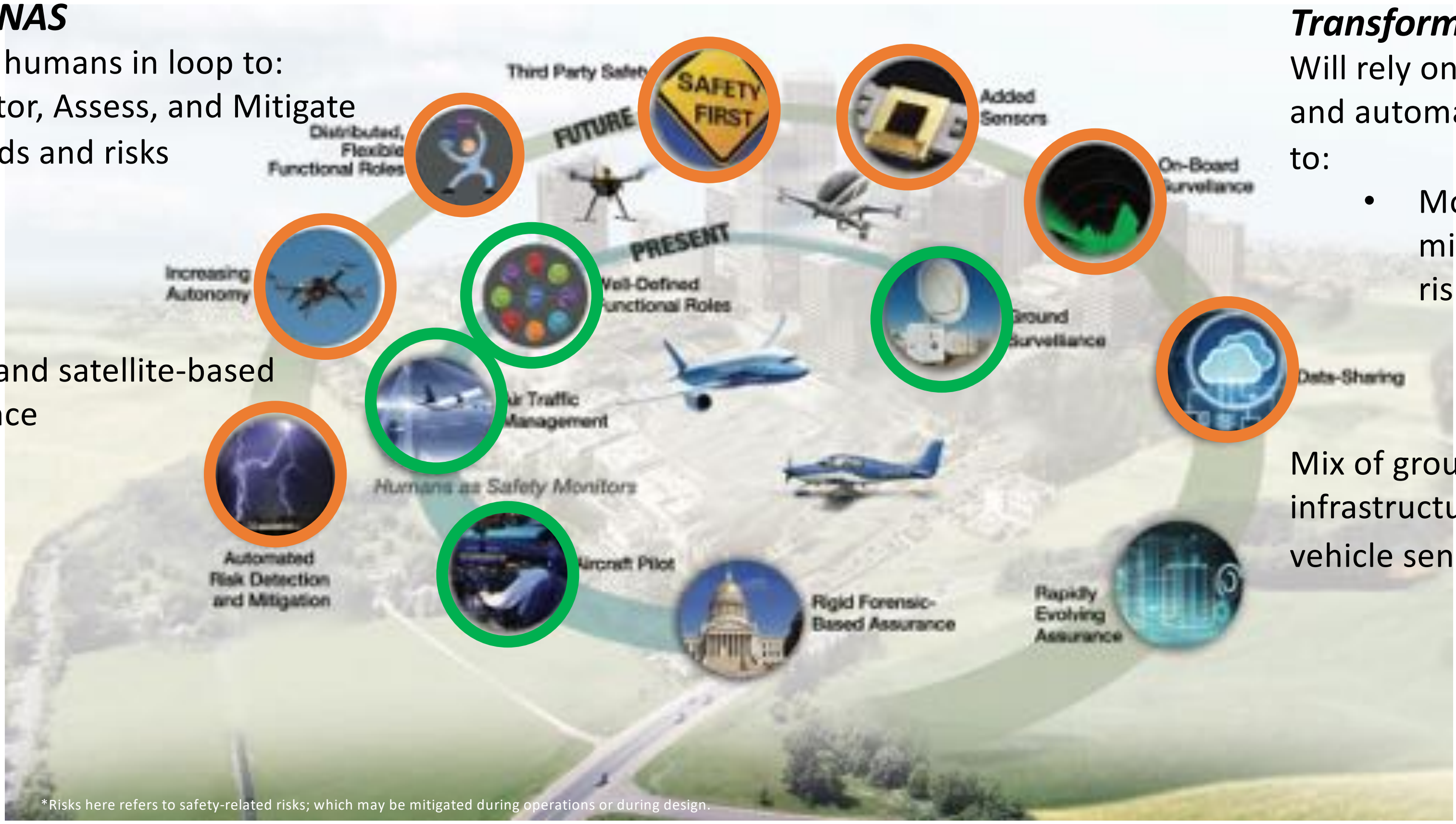
Executive Summary
Top Down Strategy – Operational Safety

Current NAS

Relies on humans in loop to:

- Monitor, Assess, and Mitigate hazards and risks

Ground- and satellite-based surveillance



FUTURE
Third Party Safety
SAFETY FIRST
Added Sensors
Distributed, Flexible Functional Roles
On-Board Surveillance
PRESENT
Increasing Autonomy
Well-Defined Functional Roles
Ground Surveillance
Data-Sharing
Air Traffic Management
Humans as Safety Monitors
Automated Risk Detection and Mitigation
Aircraft Pilot
Rigid Forensic-Based Assurance
Rapidly Evolving Assurance

*Risks here refers to safety-related risks; which may be mitigated during operations or during design.

Transformed NAS

Will rely on new data/sensors and automation or autonomy to:

- Monitor, assess and mitigate hazards and risks

Mix of ground-based, infrastructure-embedded, and vehicle sensor payloads.

System Wide Safety

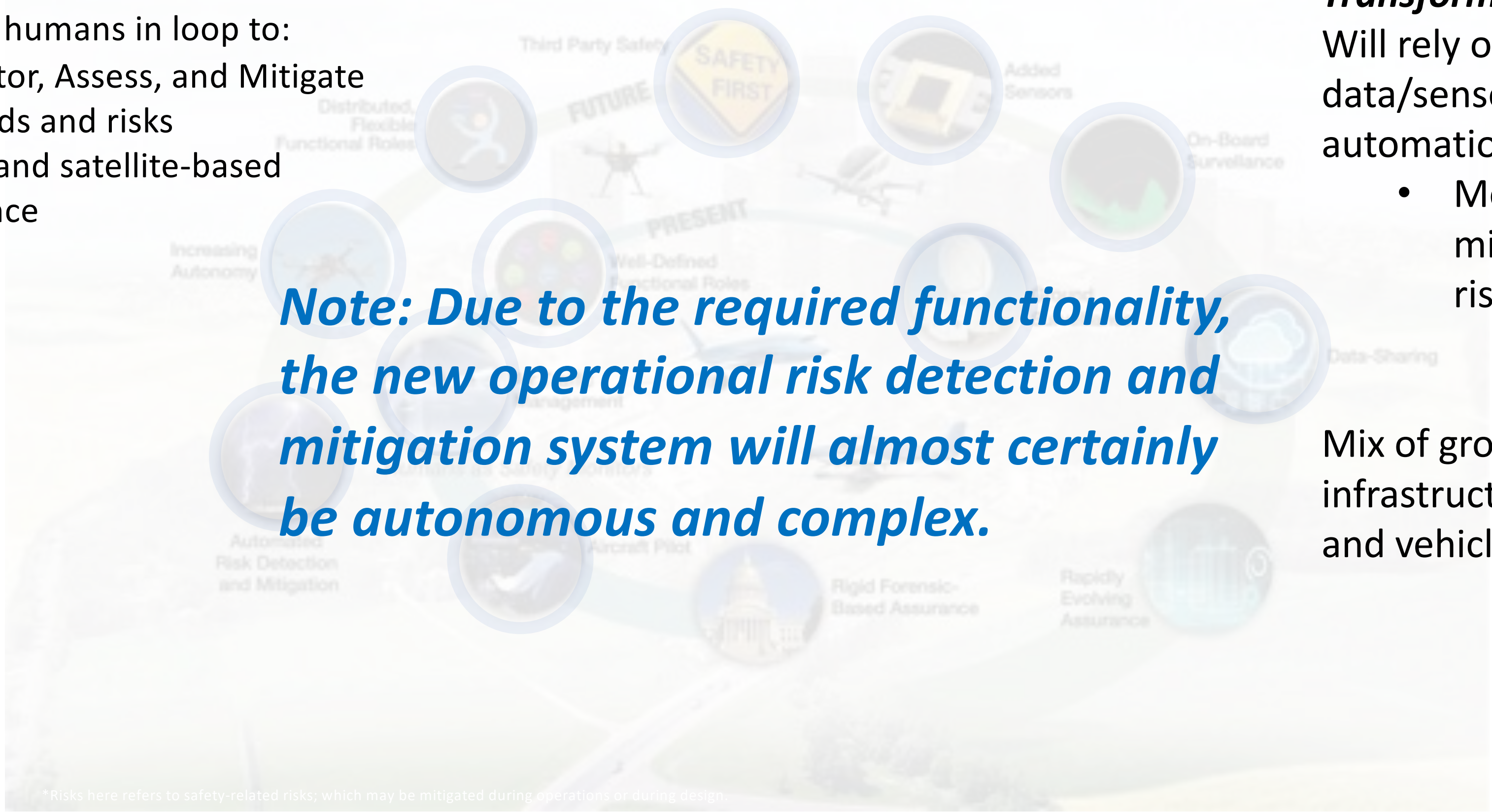
Executive Summary
Top Down Strategy – Operational Safety

Current NAS

Relies on humans in loop to:

- Monitor, Assess, and Mitigate hazards and risks

Ground- and satellite-based surveillance


Third Party Safety
SAFETY FIRST
FUTURE
Added Sensors
Distributed, Flexible Functional Roles
On-Board Surveillance
PRESENT
Increasing Autonomy
Well-Defined Functional Roles
Data-Sharing
Management
Automated Risk Detection and Mitigation
Aircraft Pilot
Rigid Forensic-Based Assurance
Rapidly Evolving Assurance

Note: Due to the required functionality, the new operational risk detection and mitigation system will almost certainly be autonomous and complex.

Transformed NAS

Will rely on new data/sensors and automation or autonomy to:

- Monitor, assess and mitigate hazards and risks

Mix of ground-based, infrastructure-embedded, and vehicle sensor payloads.

*Risks here refers to safety-related risks; which may be mitigated during operations or during design.

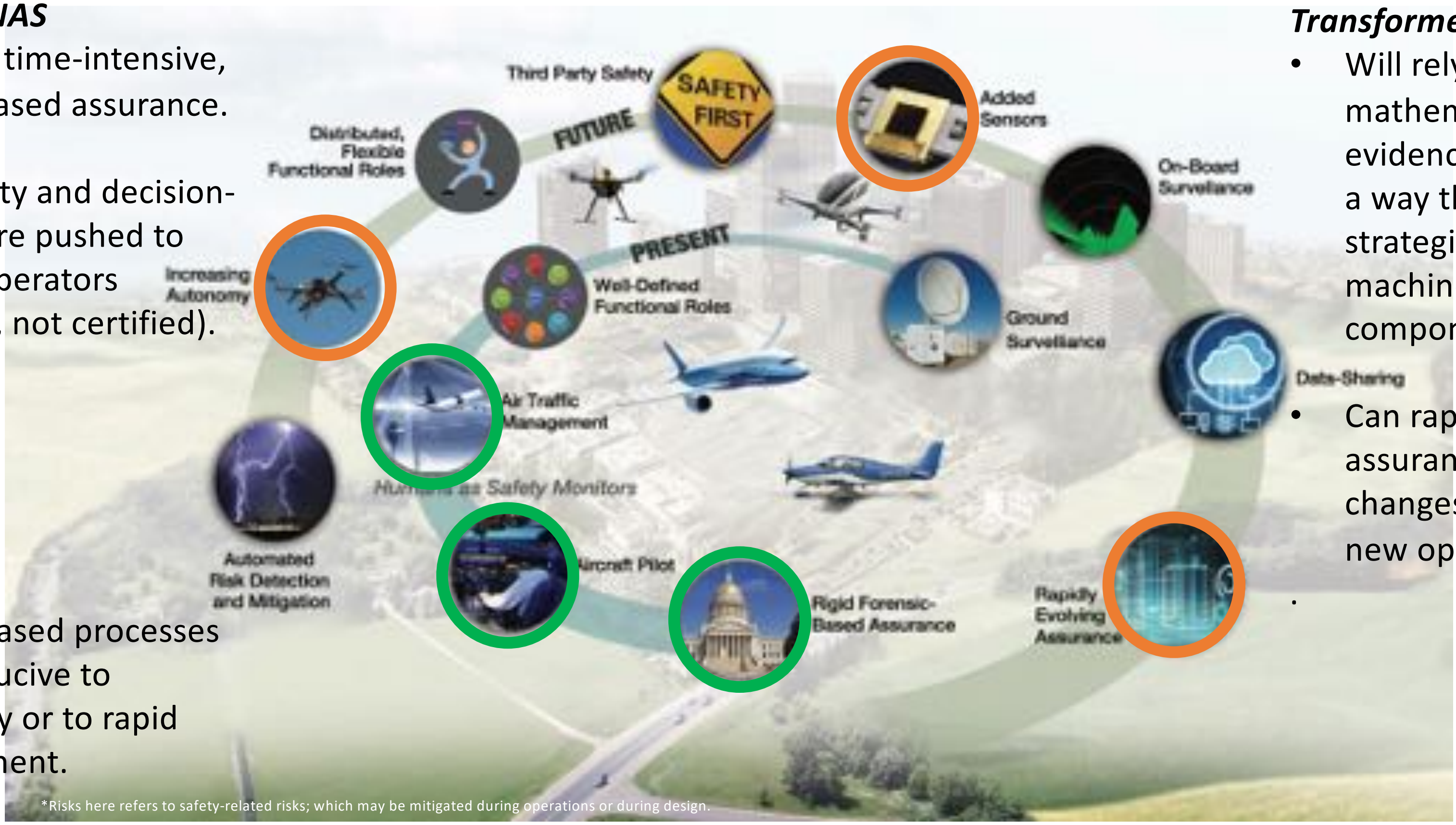
System Wide Safety

Executive Summary
Top Down Strategy – Design Safety

Current NAS
Relies on time-intensive, testing-based assurance.

Complexity and decision-making are pushed to human operators (licensed, not certified).

Testing-based processes not conducive to autonomy or to rapid development.



Third Party Safety
SAFETY FIRST
FUTURE
Added Sensors
Distributed, Flexible Functional Roles
On-Board Surveillance
PRESENT
Increasing Autonomy
Well-Defined Functional Roles
Ground Surveillance
Data-Sharing
Air Traffic Management
Humans as Safety Monitors
Automated Risk Detection and Mitigation
Aircraft Pilot
Rigid Forensic-Based Assurance
Rapidly Evolving Assurance

*Risks here refers to safety-related risks; which may be mitigated during operations or during design.

Transformed NAS
- Will rely on automated, mathematically-proven and evidence-based assurance in a way that allows the strategic and low-risk use of machine-learning enabled components.
- Can rapidly determine the assurance impact of design changes, new vehicles and new operations.

.

System Wide Safety

Future Operational Time Safety

Supports the 2025-2035 NASA Aeronautics Research Mission Directorate (ARMD) In-Time System Wide Safety Assurance (Thrust 5) Vision by early analysis and prototyping of operational safety services that

- ❑ monitor for
  - ❑ known risks and
  - ❑ anomalies that may become risks/threats,
- ❑ assess overall risks and look for hazard precursors and safety trends, and
- ❑ mitigate risks/hazards, either by
  - ❑ alerting an operator, or
  - ❑ automatically taking an action to mitigate risks.

System Wide Safety

Barriers to Future Operational Time Safety

- Increased variety and scale of operations means that people can no longer be the safety gatekeepers, or the people will be the bottleneck
- Automating safety monitoring assessment and mitigation requires several changes to operations and new technical solutions:
  - Increased data sharing so that all the data is available to automated decision makers
  - Increased data fusion so that decision-making algorithms have all necessary information
  - Predictive algorithms that can reach the appropriate conclusions
  - Confidence in the conclusions so that automated mitigation is possible
- There are also social barriers to achieving this vision – NASA can educate and inform for these barriers but will not directly address:
  - Privacy concerns
  - Data rights
- We partially address societal trust in automation and evidence by providing

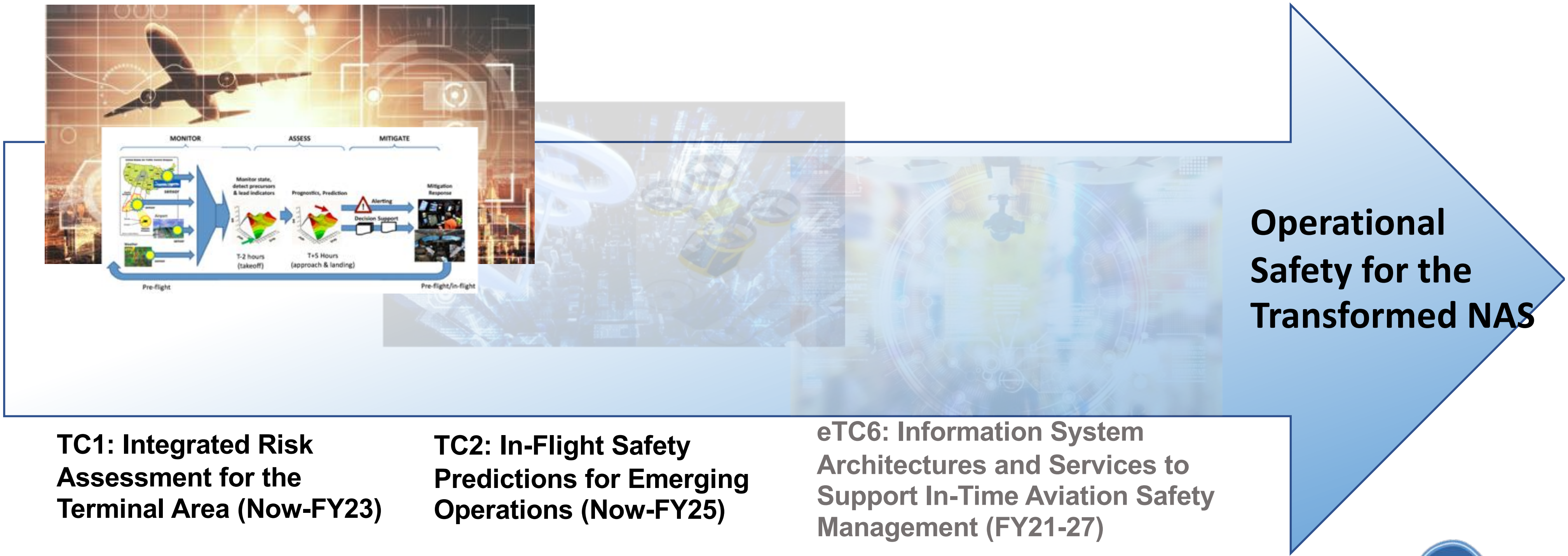
evidence for reliability in Technical Challenge 4.

System Wide Safety

Operational-Time Safety Technical Challenges

- NASA has chosen two technical challenges:
  - Integrated Risk Assessment for the Terminal Area
    - Demonstrates data fusion and automated risk analysis benefits and costs in a domain where the data currently exists
    - NASA has demonstrated expertise and leadership in this domain
    - NASA has airline partners who want these capabilities and are willing to share necessary data and dedicate resources for a cost-benefit analysis
  - In-Flight Safety Predictions for Emerging Operations
    - Increased levels of autonomy will happen with small UAS first because of mission risk profiles
    - Many emerging entrants do not realize that our current level of aviation safety is due to forensic analysis, and that accidents can kill an emerging market. NASA is a trusted intermediary between industry and the regulators.
    - NASA is the best vector for making sure that safety is an inherent part of UTM
    - Operational safety techniques for UTM are immediately applicable for UAM

In-Time System-Wide Safety Assurance



Operational Safety for the Transformed NAS

TC1: Integrated Risk Assessment for the Terminal Area (Now-FY23)

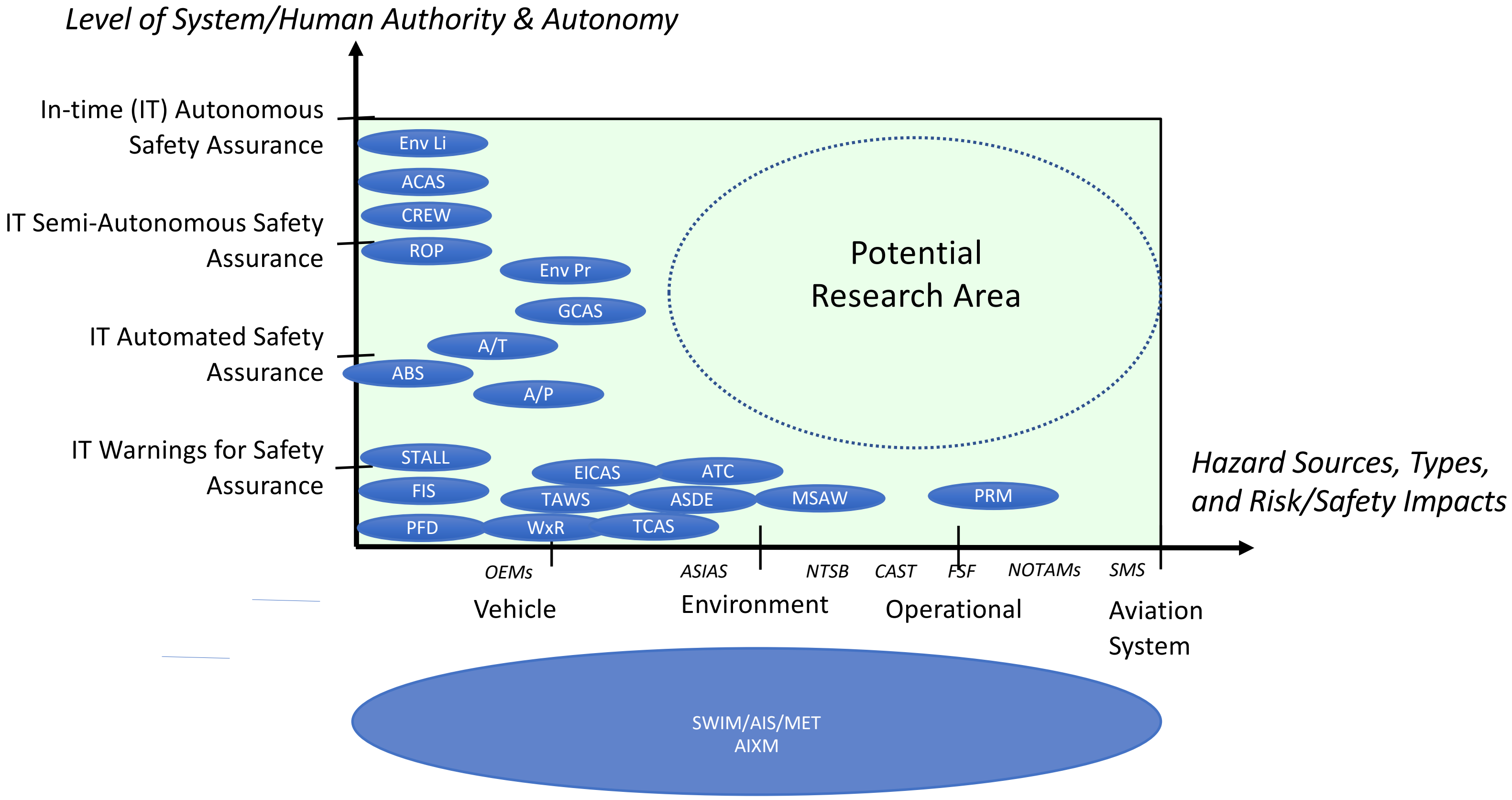
TC2: In-Flight Safety Predictions for Emerging Operations (Now-FY25)

eTC6: Information System Architectures and Services to Support In-Time Aviation Safety Management (FY21-27)

We start by working with our airline partners to build out ISSA capabilities (monitor and assess) in the terminal area, where we have the data available and can produce immediate societal benefit.

System Wide Safety

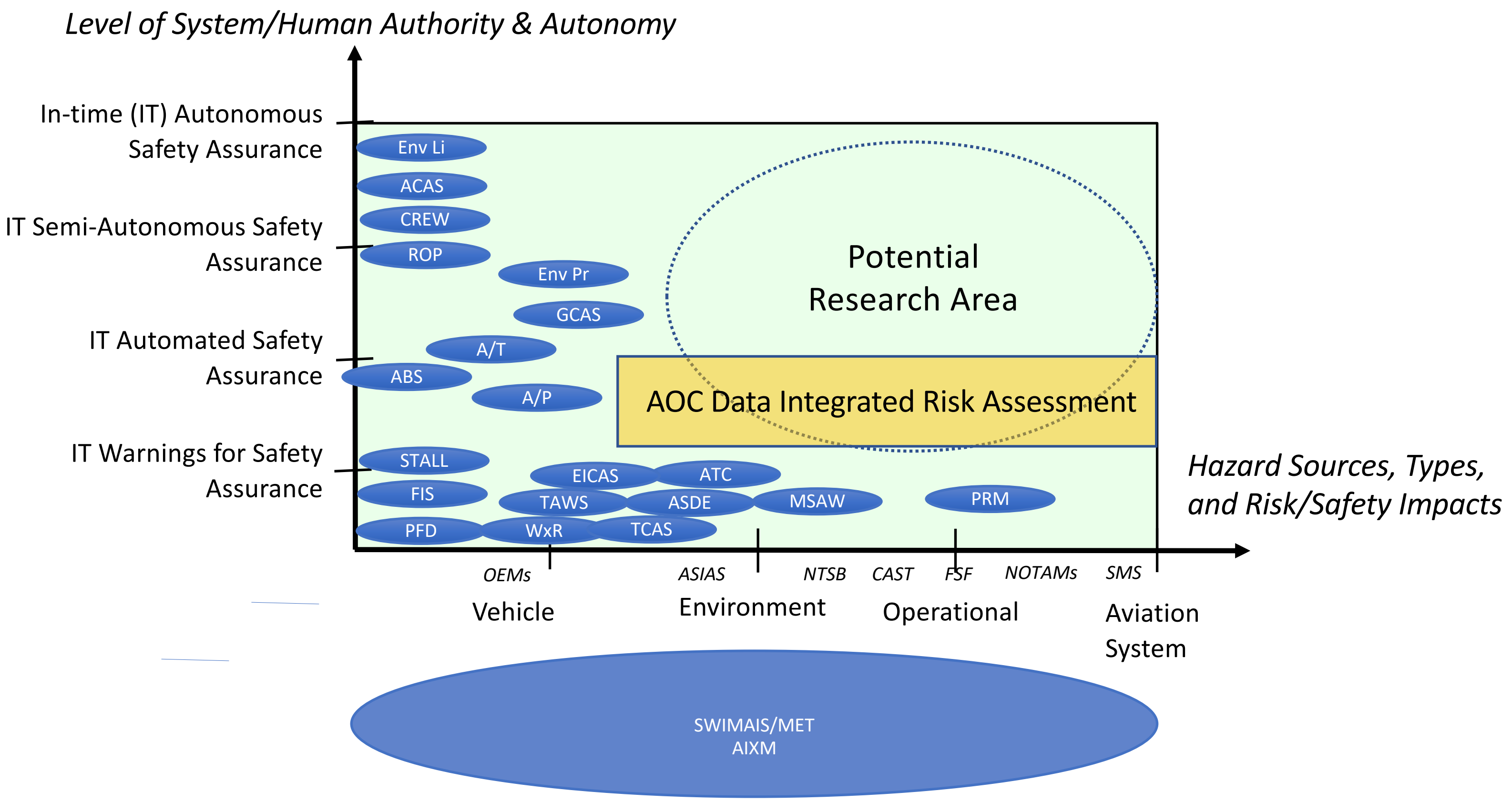
TC1: Integrated Risk Assessment for the Terminal Area What Currently Exists



Level of System/Human Authority & Autonomy
In-time (IT) Autonomous Safety Assurance
IT Semi-Autonomous Safety Assurance
IT Automated Safety Assurance
IT Warnings for Safety Assurance
Env Li
ACAS
CREW
ROP
Env Pr
GCAS
A/T
ABS
A/P
STALL
FIS
PFD
EICAS
ATC
TAWS
ASDE
MSAW
PRM
WxR
TCAS
Potential Research Area
Hazard Sources, Types, and Risk/Safety Impacts
OEMs
ASIAS
NTSB
CAST
FSF
NOTAMs
SMS
Vehicle
Environment
Operational
Aviation System
SWIM/AIS/MET
AIXM

System Wide Safety

TC1: Integrated Risk Assessment for the Terminal Area
TC1's Research Area


Level of System/Human Authority & Autonomy
In-time (IT) Autonomous Safety Assurance
IT Semi-Autonomous Safety Assurance
IT Automated Safety Assurance
IT Warnings for Safety Assurance
Env Li
ACAS
CREW
ROP
Env Pr
GCAS
A/T
ABS
A/P
Potential Research Area
AOC Data Integrated Risk Assessment
STALL
FIS
PFD
EICAS
ATC
TAWS
ASDE
MSAW
PRM
WxR
TCAS
Hazard Sources, Types, and Risk/Safety Impacts
OEMs
ASIAS
NTSB
CAST
FSF
NOTAMs
SMS
Vehicle
Environment
Operational
Aviation System
SWIMAIS/MET
AIXM

System Wide Safety

TC1: Integrated Risk Assessment for the Terminal Area

- Current System
  - Risk Assessment done by individual categories
  - Any integration of risk is accomplished by humans, based on experience
  - Human inability to evaluate all of the data streams
- Future System
  - Must be able to receive and analyze multiple streams of heterogeneous data
  - Requirement to fuse data
  - Requirement to analyze data, identify anomalies and precursors to elevated risk
  - Must provide an integrated system-level risk assessment

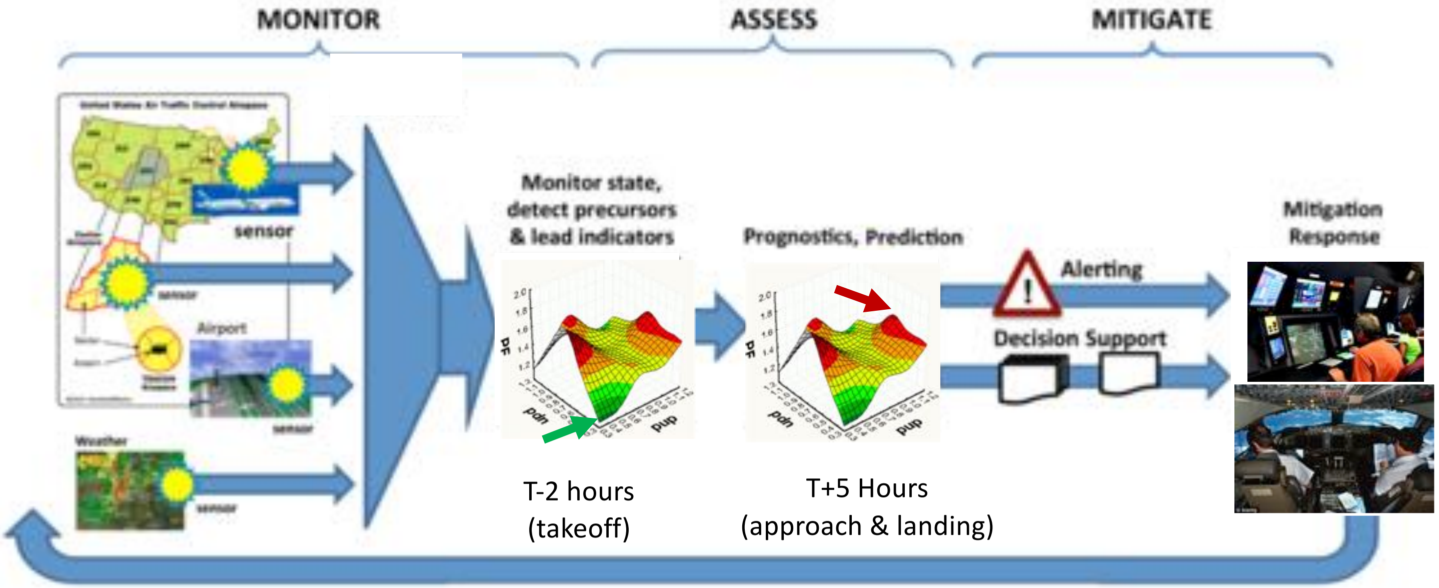
System Wide Safety

TC1: Integrated Risk Assessment for the Terminal Area

Integrated risk assessment approach

Potential early benefit for AOC/Dispatch

- Integrated risk assessment can provide improved awareness of risks over assessment of individual risks
- In-time horizon = hours



T-2 hours (takeoff)

T+5 Hours (approach & landing)

Pre-flight

Pre-flight/in-flight

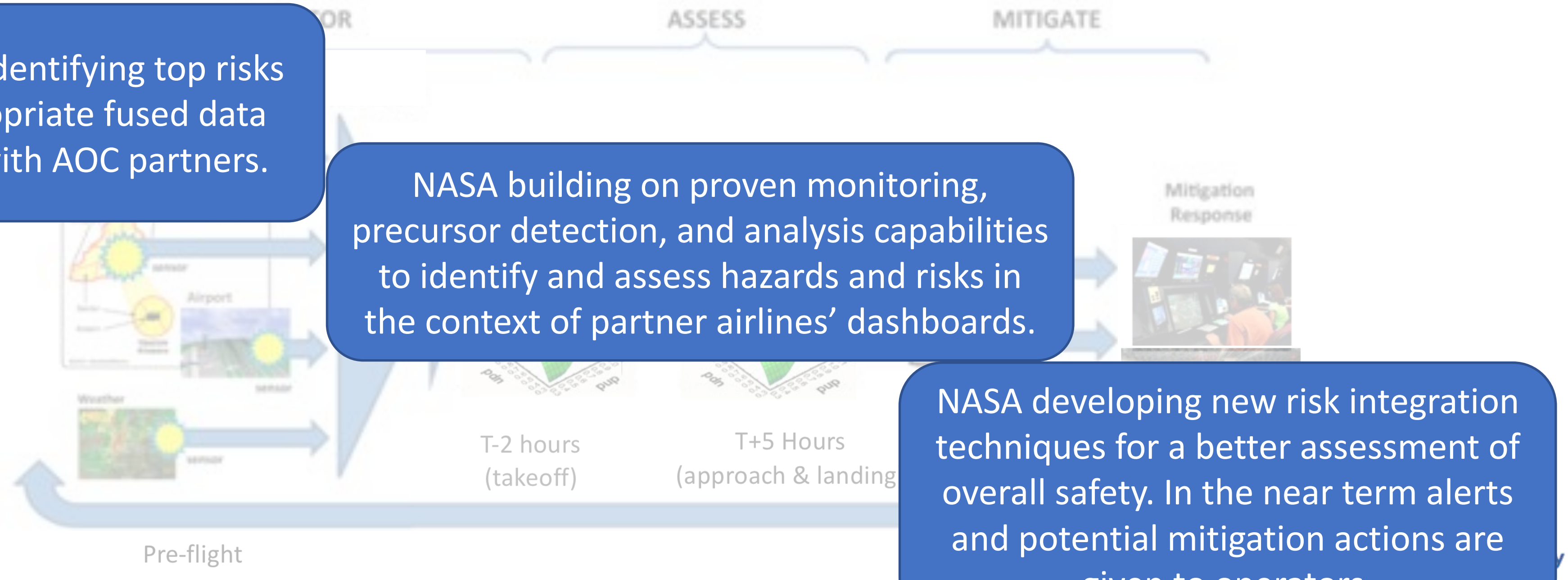
System Wide Safety

TC1: Integrated Risk Assessment for the Terminal Area

Integrated risk assessment approach

Potential early benefit for AOC/Dispatch

- Integrated risk assessment can provide improved awareness of risks over assessment of individual risks
- In-time horizon = hours



Currently identifying top risks and appropriate fused data streams with AOC partners.

NASA building on proven monitoring, precursor detection, and analysis capabilities to identify and assess hazards and risks in the context of partner airlines' dashboards.

NASA developing new risk integration techniques for a better assessment of overall safety. In the near term alerts and potential mitigation actions are given to operators.

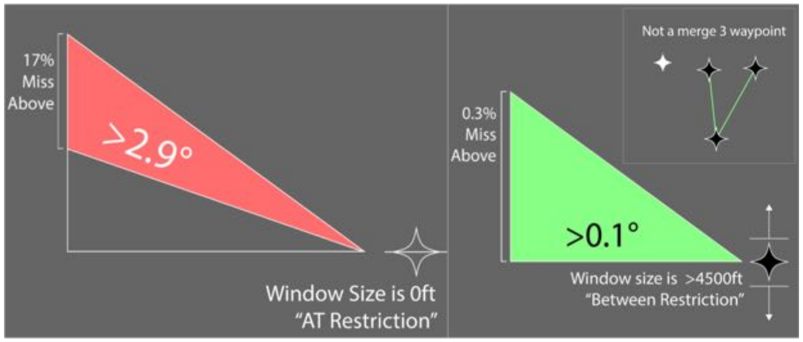
TC1: Integrated Risk Assessment for the Terminal Area

- NASA has a proven capability of developing Machine Learning algorithms that can identify anomalies in large amounts of data
- There is an industry pull from multiple airline partners to incorporate this technology and develop an overall airline safety status.
  - This work is a touchpoint for continued engagement with CAST and JIMDAT
- The development of this technology is foundational for the emerging market (TC-2 and eTC-6) but also provides an important deliverable to our traditional partners.

TC1: Integrated Risk Assessment for the Terminal Area (Now-FY23)

Progress to Date

Domain Expert Comments	Vis-Appr	High Energy	Low Energy	Late Config	Poor Tech
Low Airspeed and high AOA 5 nm from TD	X		X		
Low Airspeed and high AOA 6 nm from TD.	X		X		
Well above Glideslope at 28 nm from TD becomes below GS at 9 nm from TD.	X		X		
Captured Glideslope from above	X				X
Low Airspeed and high AOA inside 5 nm from TD	X		X		
Fast at 10 nm from Touchdown	X	X		X	
High rate of descent 14 nm from TD.	X				
High Airspeed and intercepts Glideslope 3 nm from TD.	X	X		X	
Fast airspeed, too fast to extend flaps 5 nm from TD. "…behind the airplane."	X	X			X
Below Glideslope 10 nm from TD	X		X		



We are developing capabilities in advance of final agreements with airline partners.

Toolsuite that finds operationally significant hazards in data is being validated and improved through collaboration with ASIAS/MITRE:

- MITRE SME has examined top 40 'most anomalous' events and determined 10 were operationally significant.
- These 10 were used to train a classifier, which then found two more operationally significant events in the ASIAS data

Capability to fuse aircraft data (e.g. trajectories and weather data) and use trees to automatically find precursors is being validated and improved using Sherlock/ATM Data Warehouse

- Capability automatically determined which precursors were most likely to predict that aircraft would fail to adhere to RNAV, and also which precursors would predict strict adherence

Each of these accomplishments are transferrable to integrated risk assessment for US Airlines Operation Centers as soon as the agreements are finalized.

In-Time System-Wide Safety Assurance

MONITOR
ASSESS
Monitor state, detect precursors & lead indicators
Prognostics, Prediction
T-2 hours (takeoff)
T+5 Hours (approach & landing)
Pre-flight

Operational Safety for the Transformed NAS

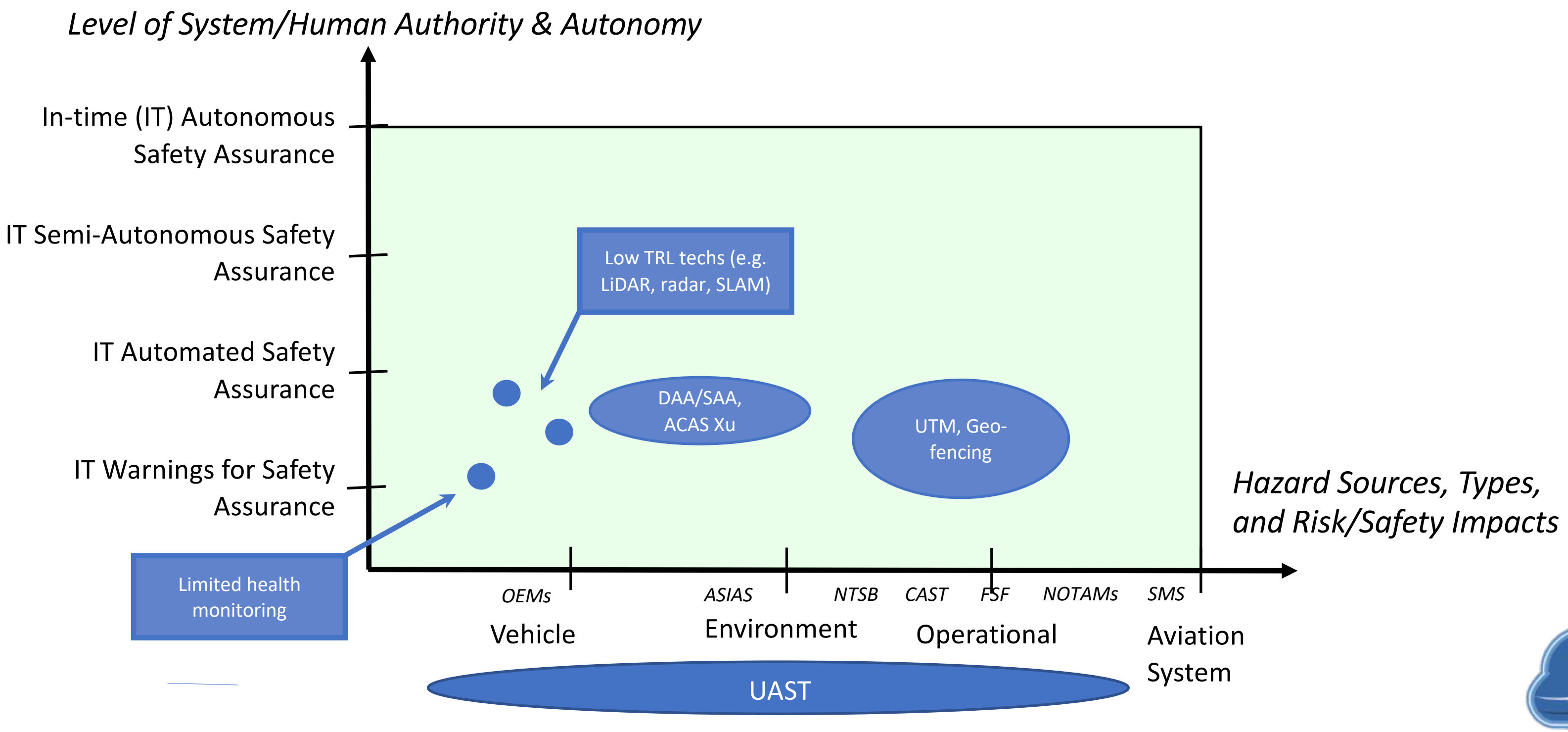
TC1: Integrated Risk Assessment for the Terminal Area (Now-FY23)

TC2: In-Flight Safety Predictions for Emerging Operations (Now-FY25)

eTC6: Information System Architectures and Services to Support In-Time Aviation Safety Management (FY21-27)

Using what we learn in TC1, in addition to work that we've already begun with sUAS and UTM, we continue to understand the risks and hazards associated with aviation emerging operations, and NASA will make recommendations to UAST and the FAA for minimum data requirements and standards necessary to monitor, assess, and mitigate for safety.

TC2: In-Flight Safety Predictions for Emerging Operations What Currently Exists



Level of System/Human Authority & Autonomy
In-time (IT) Autonomous Safety Assurance
IT Semi-Autonomous Safety Assurance
IT Automated Safety Assurance
IT Warnings for Safety Assurance
Low TRL techs (e.g. LiDAR, radar, SLAM)
DAA/SAA, ACAS Xu
UTM, Geo-fencing
Limited health monitoring
Hazard Sources, Types, and Risk/Safety Impacts
OEMs
ASIAS
NTSB
CAST
FSF
NOTAMs
SMS
Vehicle
Environment
Operational
Aviation System
UAST

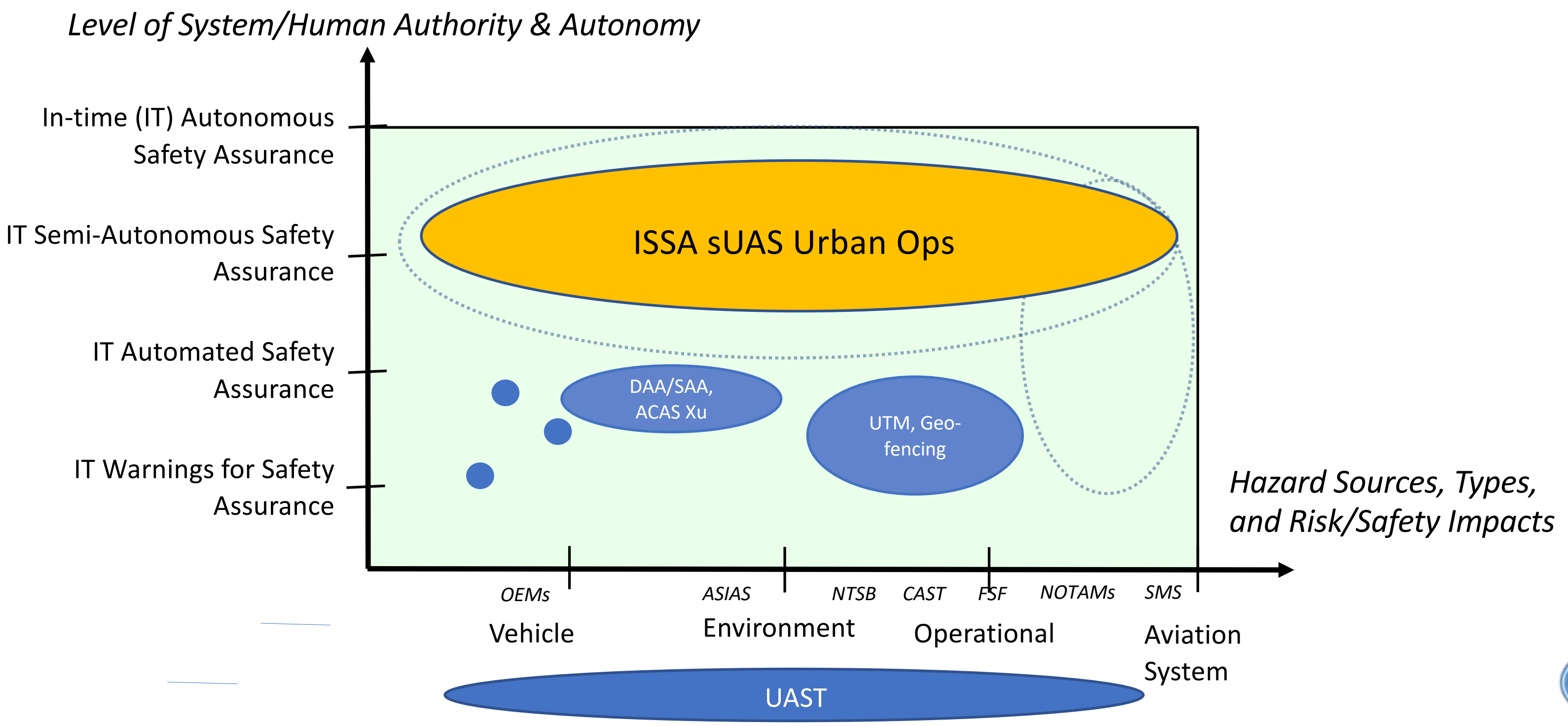
System Wide Safety

TC2: In-Flight Safety Predictions for Emerging Operations

- Current System
  - No overall predictive safety system exists
  - UTM research and development has become the de-facto industry standard for future system architecture
- Future System
  - Predicted density of sUAS urban operations require a robust ability to understand system safety
  - TC-2 is the first demonstration of an ISSA capability in an urban sUAS environment
    - Using UTM architecture allows insight into requirements for UTM inspired ATM

System Wide Safety

TC2: In-Flight Safety Predictions for Emerging Operations
TC2's Research Space



Level of System/Human Authority & Autonomy
In-time (IT) Autonomous Safety Assurance
IT Semi-Autonomous Safety Assurance
IT Automated Safety Assurance
IT Warnings for Safety Assurance
ISSA sUAS Urban Ops
DAA/SAA, ACAS Xu
UTM, Geo-fencing
Hazard Sources, Types, and Risk/Safety Impacts
OEMs
ASIAS
NTSB
CAST
FSF
NOTAMs
SMS
Vehicle
Environment
Operational
Aviation System
UAST

System Wide Safety

TC2: In-Flight Safety Predictions for Emerging Operations

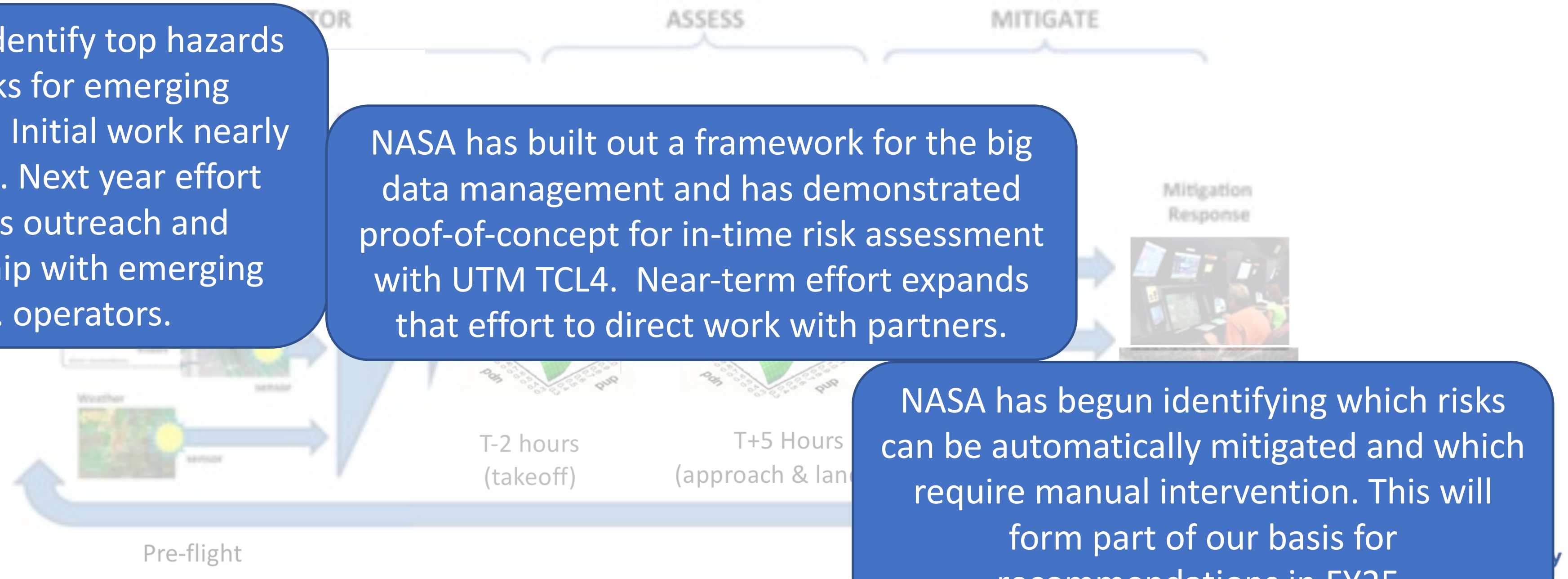
- NASA's previous and current research positions it well to participate in this work.
  - Foundational work in data fusion and analysis TC-1
  - UTM research & development
  - Role in UAST
  - Direction of future ARMD portfolio
- Developing partnerships allow NASA to leverage and deploy its work
  - USGS
  - Nuro
  - Google Loon
  - Bell Helicopter
  - Others?

TC2: In-Flight Safety Predictions for Emerging Operations

Technical Approach

Potential early benefit for AOC/Dispatch

- Integrated risk assessment can provide improved awareness of risks over assessment of individual risks
- In-time horizon = hours

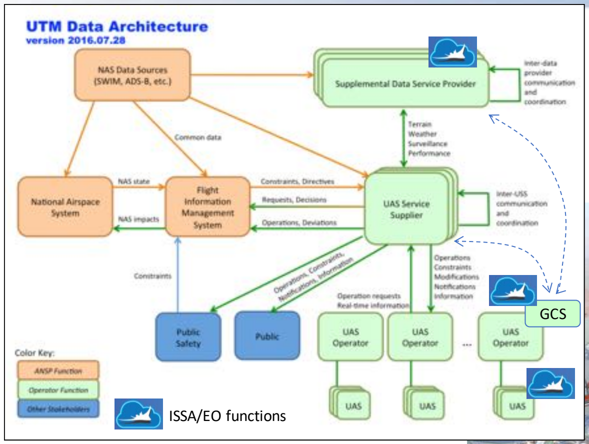


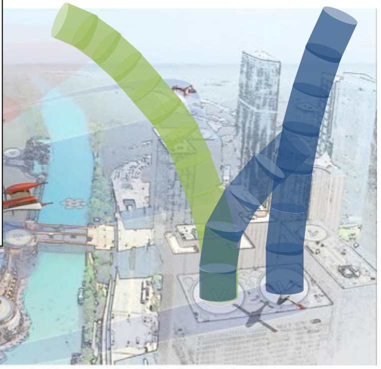
Monitor: Identify top hazards and risks for emerging operations. Initial work nearly complete. Next year effort includes outreach and partnership with emerging U.S. operators.

NASA has built out a framework for the big data management and has demonstrated proof-of-concept for in-time risk assessment with UTM TCL4. Near-term effort expands that effort to direct work with partners.

NASA has begun identifying which risks can be automatically mitigated and which require manual intervention. This will form part of our basis for recommendations in FY25.

TC2 Progress Summary



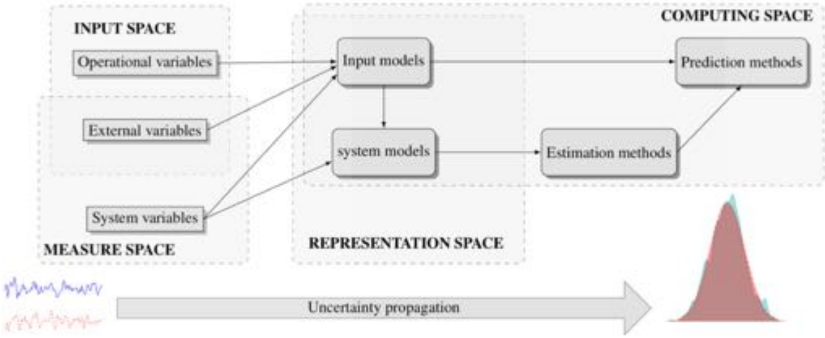


Uncertainty management framework (in Thrust 5 Roadmap and NRC Thrust 5 report) is complete. Will be published in Aviation 2019 and other venues.

Three initial safety service prototypes developed: battery metric, proximity metric, casualty risk metric.

- Demonstrated as part of TCL4.
- Also will be integrated into ATM-X Testbed for simulations and GC.

Demonstrations will validate the data and information requirements due this year. (API 19-4)



System Wide Safety

TC2: Uncertainty Management Framework

(ISSA/EO – In-time System-wide Safety Assurance for Emerging Operations)

Motivation and Objective

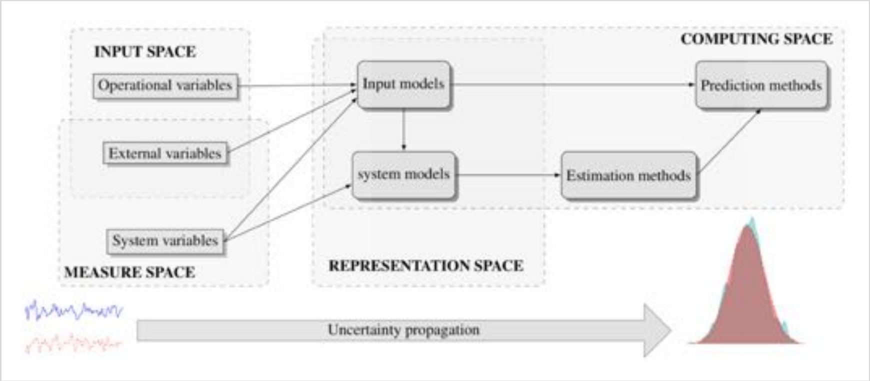
ISSA/EO promotes data-driven predictive capabilities that (1) enable timely mitigation of safety risks; and (2) consider the complex interplay of many factors that are difficult to measure or track. Predictive capabilities can be misleading if their limitations are not well understood and accounted for.

Milestone SWS.EO-1.3 (falls directly from the Thrust 5 roadmap):

- Develop a framework for uncertainty management
- Exit criteria – Describe a method for encapsulating uncertainty from sources used to estimate, track, and predict safety/risks; Method includes approaches to uncertainty representation, characterization, and assessment of propagation of effects

Approach

- Accommodate both Bayesian and non-Bayesian methodologies
- Consider propagation through ISSA/EO functional elements
- Consider source types (models, measurements, input, etc.)
- Trajectory prediction function used as exemplar test case
- Simulation and flight data used to confirm framework validity
- (Next step) Apply to other ISSA/EO predictive functions and refine



Accomplishment

- Achieves milestone SWS.EO-1.3 (Q2/FY19)
- Becomes basis to develop/evaluate all ISSA predictive functions
- Helps to establish information requirements (API AR-4, Q4/FY19)
- Helps to ID uncertainty sources & effects on safety metric estimates
- All documentation, incl. sim and flight test data archived internally
- Publication: “Real-time UAV trajectory prediction for safety monitoring in low-altitude airspace” AIAA AVIATION, 06-2019

  (3 others submitted or planned)

System Wide Safety

Contributors: Corbetta, Banerjee, Okolo, Gorospe, and Luchinsky (NASA ARC)

TC2: UTM TCL4 Engagement with Airspace Operations Lab (AOL) Simulations

(ISSA/EO – In-time System-wide Safety Assurance for Emerging Operations)

Motivation and Objective

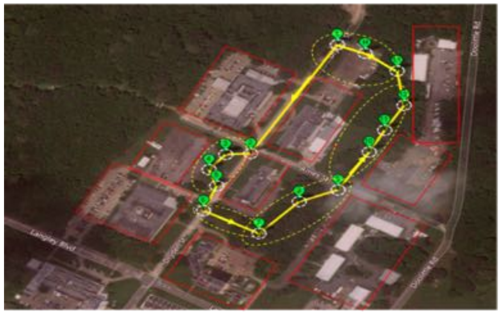
In line with the ISSA/EO (TC-2) research agenda, to carry out extensive set of simulations that encompass coordinated tracking of safety metrics, we participated in a number of "Sprint" activities held by the UTM project in preparation for the TCL4 flight demonstrations.

SWS TC2 researchers engaged in both "Sprint 3" and "Sprint 4" activities in the NASA Ames Airspace Operations Lab (AOL) with the objective of proving out UTM integration and testing the SWS SDSP (Supplemental Data Service Provider) interface.

Approach & Accomplishments

- Integration leading up to both Sprint activities included:
- Participation by AOL researchers to enable integration of systems and development of AOL simulation tools
- Developed simulation data for a region of airspace in Langley, Virginia.
- Development of backend SWS processes to handle simulation requests. Debug and test of interaction through the REST interface.
- Collaboration with UTM and AOL researchers for participation in planned activities during Sprint3 and Sprint4 tests
- GUI interface design and development for display of in-time safety metric responses

SWS/UTM/AOL Real-time Integration



Impacts

- Achieves milestone SWS.EO-2.2: 2nd-gen capability simulation and/or flight tests (initial safety margin tracking)
- Executed the simulated flight path in concert with other Sprint3/Sprint4 participants
- Proved data collection and safety metric calculation by the SWS SDSP
- Presented the in-time safety metric outputs to the user in the AOL lab
- Internal Report: "UTM Sprint 3 Participation – SWS TC2 SDSP" and "UTM Sprint 4 Participation – SWS TC2 SDSP"

Next Steps

- Joint flight testing at Langley; TC2 analysis of TCL4 flight data from participants.

System Wide Safety

TC2: Architecture and Information Requirements

(ISSA/EO – In-time System-wide Safety Assurance for Emerging Operations)

Objective

Annual Performance Indicator (API AR 19-4) (Sep 30, 2019):

"Identify data architecture and information requirements (i.e., content and quality) for in-time monitoring of selected operational risks for small Unmanned Aircraft Systems (sUAS)"

- Identification of three safety risks and the data requirements for monitoring those risks, demonstrating how risk can be identified using the available data (To achieve **GREEN** Rating).

Approach

: Architecture – Presume UTM ecosystem; Identify how ISSA functions can overlay (e.g. 'Supplemental Data Services')

: Information requirements – Consider content, quality, and exchange; Use existing standards where able and as guide; Assume monitoring for 5 high priority safety risks

: Validation – Use simulation and flight testing to (1) confirm architecture support, and (2) expose previously-unknown info req'ts (e.g. incl. 3 safety risk services within UTM SDSP construct); partner to leverage/access larger data sets

: Documentation – Baseline (FY19), Revisions (FY20+), Informing FAA/industry standards (e.g. via RTCA, UAST, RTT(s))

Progress

: Status – On schedule

: Architecture & functions defined

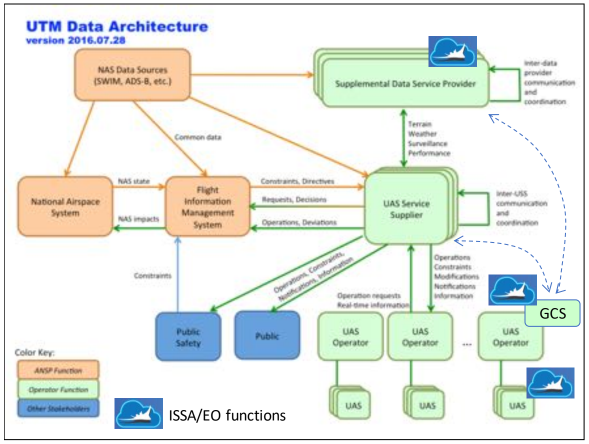
: Sims completed (w UTM Sprints)

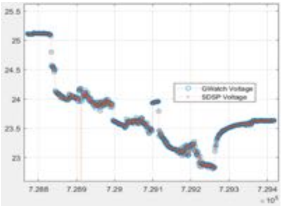
: Gen-1 flight tests completed (Dec); Gen-2 underway*

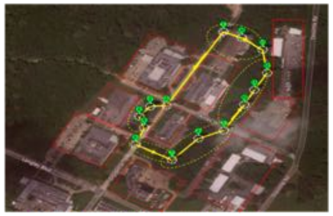
: Initial evaluation of 3 'services'

: Data collected to advance others

: Info reqm'ts doc drafted to organize as 'all in one place'







Next Steps

- Aligning with UAM Domain (via ATM-X collaboration)
- RTCA request for info on UAM/sUAS data needs
- Inputs to UAST Data WG Action Plans
- DHS/DoT Phase 2 (APNT)
- Nuro and NASCTNC (future)

TC2: ATM-X/UAM Integration

(ISSA/EO – In-time System-wide Safety Assurance for Emerging Operations)

Motivation and Objective

ARMD's FY 2021 Program and Resources Guidance states:

"AOSP shall assess rebalancing the SWS investments to accelerate work and better support the UAM and GC. In addition to rebalancing, AOSP should determine whether any additional budget may be required."

- The ISSA/EO (TC-2) research agenda has been adjusted to accelerate the planned FY20 UAM Decision Point (MS SWS.EO.1.7); and to begin integration immediately of the most mature and relevant elements of the ISSA/EO system concept within the developing ATM-X/GC environment.

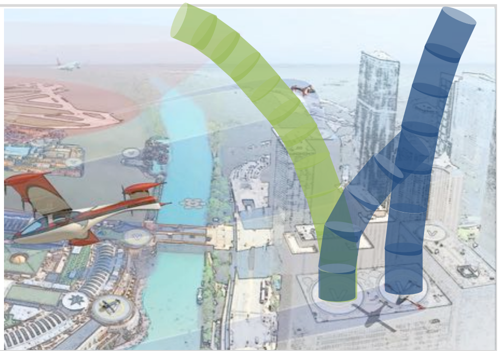
Approach

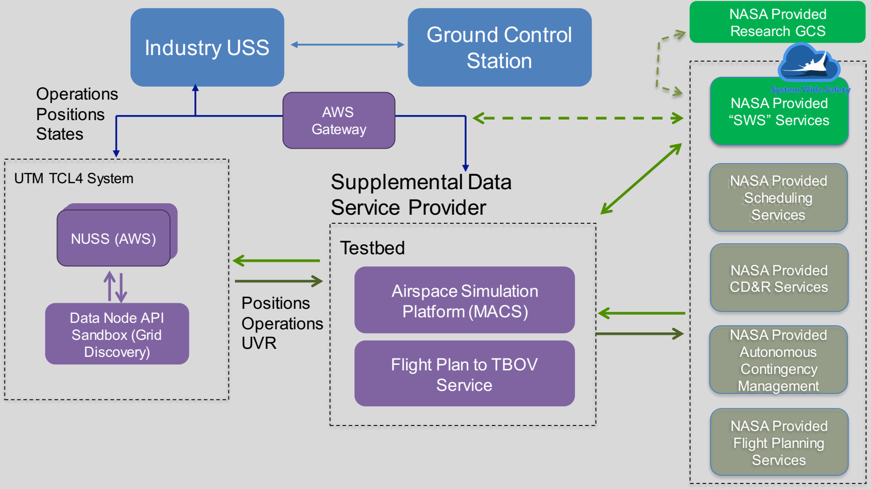
- Work to accelerate & integrate <u>3</u> 'SWS services' (initially) (X2 sim)
  - Battery prognostics; Proximity metric; Casualty risk metric*
- Collect UAM vehicle-specific and other data needed to (a) demo existing services in this domain, (b) advance other ISSA/EO services or functions, and (c) expose any new/unique requirements
- Assume ISSA/EO functions that reside within Ground Control Station or Vehicle must be tested as prev planned, or in GC2, 3, …
- Interaction with UAM community and stakeholders will allow adjustments to R&D scope and priorities moving to GC2, 3, …

*Originated within UTM project; co-developed since SWS start-up

Integration Architecture and Scenarios (X2 sim)

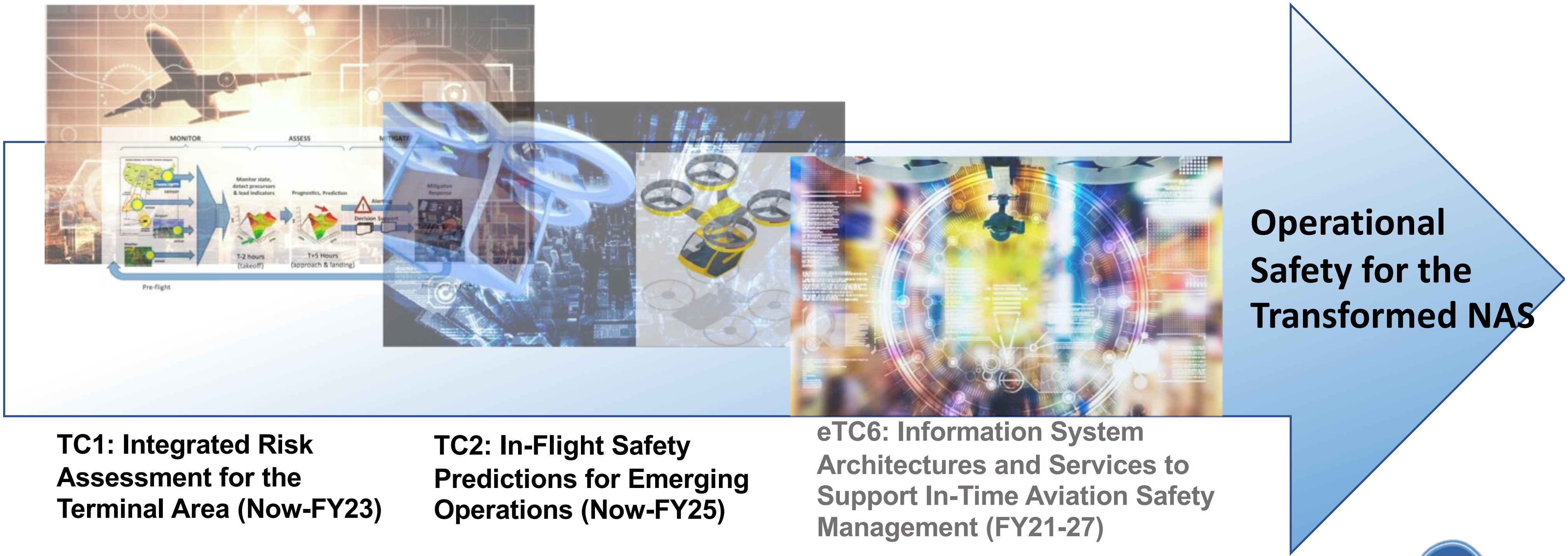
- Draft approach below
- Testing, Aug-Sep, 2019




Industry USS
Ground Control Station
NASA Provided Research GCS
Operations
Positions
States
AWS Gateway
NASA Provided "SWS" Services
UTM TCL4 System
NUSS (AWS)
Data Node API Sandbox (Grid Discovery)
Supplemental Data Service Provider
Testbed
Airspace Simulation Platform (MACS)
Flight Plan to TBOV Service
Positions
Operations
UVR
NASA Provided Scheduling Services
NASA Provided CD&R Services
NASA Provided Autonomous Contingency Management
NASA Provided Flight Planning Services

Risk: Inter-project dependencies? (Sched, resources, etc)

In-Time System-Wide Safety Assurance



Operational Safety for the Transformed NAS

TC1: Integrated Risk Assessment for the Terminal Area (Now-FY23)

TC2: In-Flight Safety Predictions for Emerging Operations (Now-FY25)

eTC6: Information System Architectures and Services to Support In-Time Aviation Safety Management (FY21-27)

Work with emerging U.S. industry partners and regulators to understand and recommend requirements and standards for an In-Time Aviation Safety Management System (IASMS) as recommended by the NRC Thrust 5 committee. Work between now and FY21 will identify gaps not currently being filled by our industry and regulatory partners.

Executive Summary
eTC6: Information System Architectures and Services to Support In-Time Aviation Safety Management (IASMS)

Challenge Objective: Define and demonstrate an information architecture and data-sharing approach to a Safety Management System for UAM-like airspace

Motivation
“The range of capabilities that can be successfully implemented in an [ISSA] concept will be limited if available data are inadequate in terms of completeness, quality, consistency, the ability to fuse them in the time scales of interest, the ability to store them for future use, and the relative cost and value of obtaining additional and/or higher quality data.” “This project is urgent because it is fundamental to the success of an IASMS and because some components will likely take years to complete.” NRC Report

Focus
SWS TC1 does foundational work demonstrating the benefit of an ISSA-like system in the current and very near-term airspace. SWS TC2 provided insight into data integrity and quality requirements for the earliest emerging markets. eTC6 uses the TC1 and TC2 work to address the larger scope of the NRC-requested IASMS.

The increased density and heterogeneity of vehicles and operations that will be brought about by AAM and UTM require a proactive consideration of risk as the system is built as opposed to a the historical reactionary approach. To fully understand tomorrow’s risks, it is necessary to drive the safety data requirements up front.

Why This Work is Prioritized
The scale, heterogeneity, and types of operations performed for UAM will require a In-Time Aviation Safety Management System (IASMS) that is more proactive and predictive than our current-day SMS (Safety Management System). As suggested by the NRC above, this work is required for UAM.

System Wide Safety

Future Design Time Safety

Supports the 2025-2035 Thrust 6 Vision: ‘Introduction of aviation systems with *flexible* autonomy based on *earned levels of trust*, capable of carrying out mission-level goals.’

System Wide Safety

Barriers to Future Design Time Safety

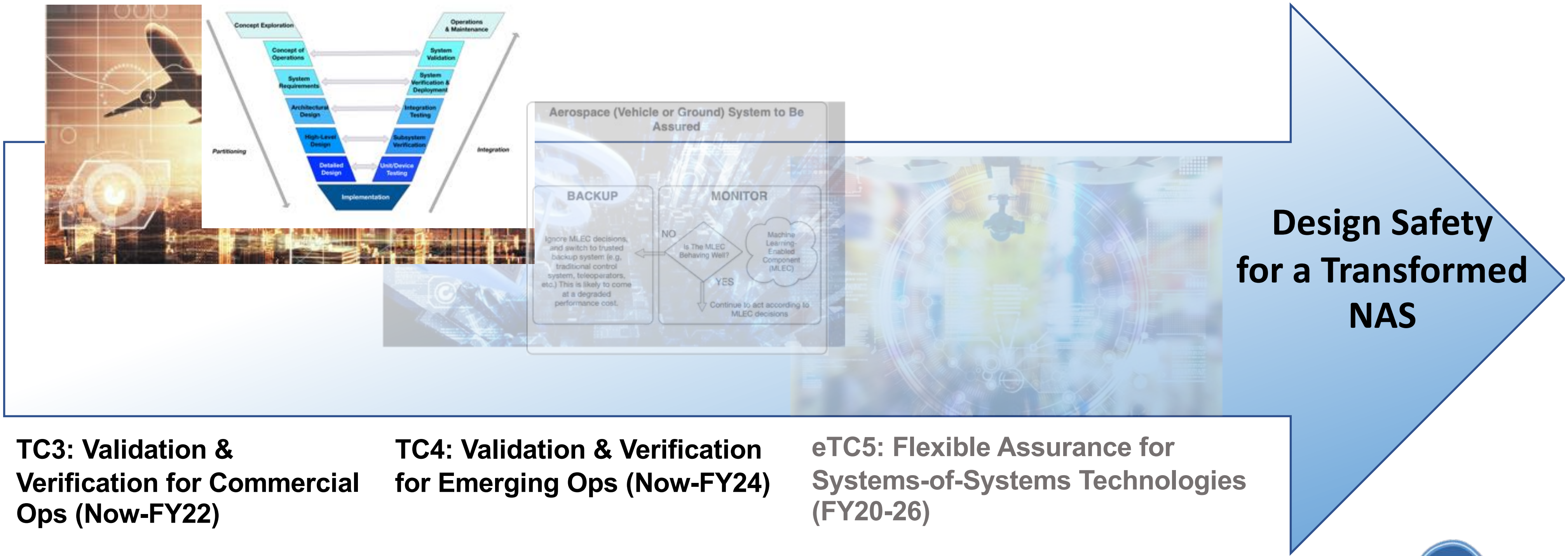
- Increased variety and scale of operations means that people can no longer be the safety gatekeepers, or the people will be the bottleneck
- Our current assurance processes assume that all decision-making (non-determinism) happens during operations, by people
  - People are licensed and trusted, hardware and software are completely exercised for assurance
  - Determinism in the hardware and software allows us to exercise them using testing
  - Recent aerospace systems, while deterministic, are complex enough that testing-based assurance has been costly
  - Changes made to components within the system have impacts throughout the system (emergent behaviors)
- There are also social barriers to achieving NASA's vision – NASA can educate and inform for these barriers but will not directly address:
  - New entrants often underestimate society's tolerance for risk
  - Trust in automation and autonomy (We partially address this in technical challenge 4)

Design-Time Safety Technical Challenges

- NASA has chosen two technical challenges:
  - V&V for Commercial Operations
    - Addresses cost barrier to implementing new aerospace systems in current regulatory framework by automating the collection of evidence and the creation of safety arguments
    - NASA has already built and released tools that are being used by industry partners
    - All that remains for this technical challenge is the collection of overall impact on assurance resources (time/cost) by industry – complete by FY22
  - Complex Autonomous Systems Assurance
    - Increased levels of autonomy will happen with small UAS first because of mission risk profiles, increased autonomy will eventually need to be a part of UAM or the large-scale business case won't close (not enough trained operators for demand).
    - Many emerging entrants do not realize that our current level of aviation safety is due to forensic analysis, and that accidents can kill an emerging market. NASA is a trusted intermediary between industry and the regulators.
    - NASA is a leader on the assurance of autonomy and is asked for help regularly by industry and by other government agencies
- Other technical challenges were considered, and are available in backup slides
- The assurance of autonomy and of complex systems has been repeatedly addressed by National Academies and expert committees for the DoD

System Wide Safety

Design Time Safety Assurance


Concept Exploration
Concept of Operations
System Requirements
Architectural Design
High-Level Design
Detailed Design
Implementation
Unit/Device Testing
Subsystem Verification
Integration Testing
System Verification & Deployment
System Validation
Operations & Maintenance
Partitioning
Integration
Aerospace (Vehicle or Ground) System to Be Assured
BACKUP
MONITOR
Ignore MLEC decisions, and switch to trusted backup system (e.g. traditional control system, teleoperators, etc.) This is likely to come at a degraded performance cost.
NO
Is The MLEC Behaving Well?
YES
Machine Learning-Enabled Component (MLEC)
Continue to act according to MLEC decisions

Design Safety for a Transformed NAS

TC3: Validation & Verification for Commercial Ops (Now-FY22)

TC4: Validation & Verification for Emerging Ops (Now-FY24)

eTC5: Flexible Assurance for Systems-of-Systems Technologies (FY20-26)

TC3 completes work NASA has done on lowering the cost and time of certification while maintaining safety. We are now using NASA-developed tools and techniques to measure the impact of the tools over the current manual processes.

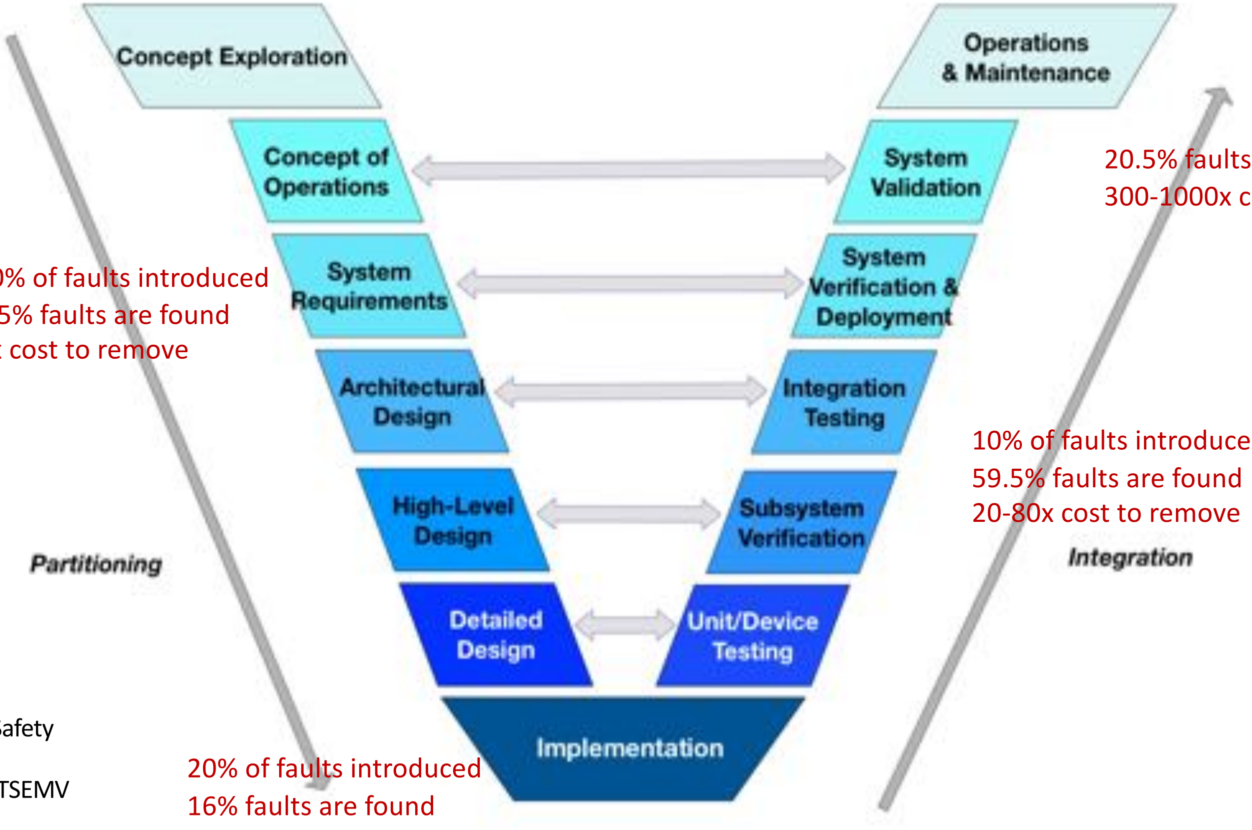
System Wide Safety

TC3: V&V for Commercial Ops (Now ends FY22)

Addressing the cost barrier

The primary cost drivers for the current assurance process are defect escapes and rework.

Industry TIMs over the last 5 years have identified <u>System Requirements</u> as the part of the life cycle in which NASA could have the most impact.



70% of faults introduced
3.5% faults are found
1x cost to remove

20.5% faults are found
300-1000x cost to remove

10% of faults introduced
59.5% faults are found
20-80x cost to remove

20% of faults introduced
16% faults are found
5x cost to remove

Source: Peter Feiler. ‘Supporting the ARP4761 Safety Assessment Process with AADL. Feb 6, 2014. https://wiki.sei.cmu.edu/aadl/images/1/13/ERTSEMV2-Feb2014.pdf

System Wide Safety

TC3: V&V for Commercial Ops (Now ends FY22)

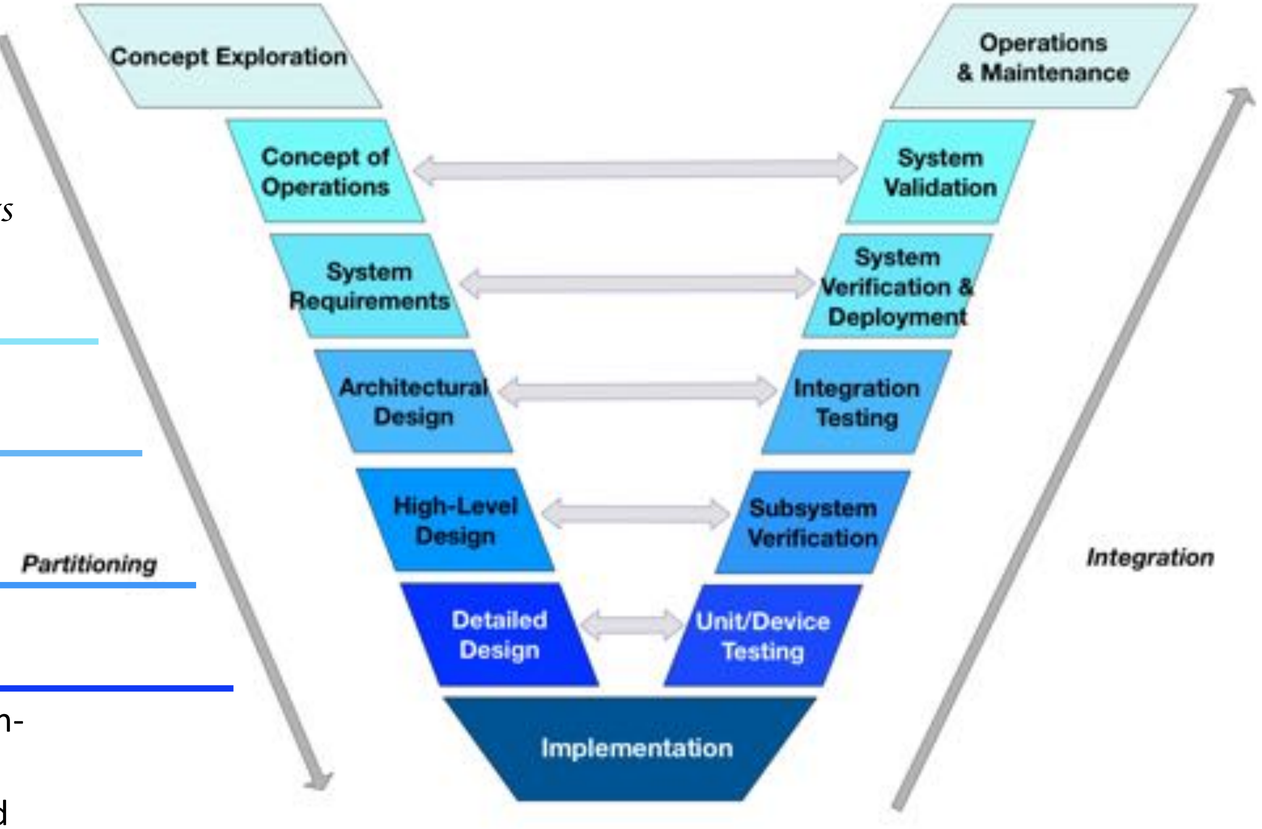
NASA-Developed Capabilities

Library of Mathematical Proofs to Validate Requirements – used for RTCA committees for compact position reporting (fixed 500 nautical-mile error in requirements) and to determine detect-and-avoid requirements

Tool to Automatically Analyze Requirements & Auto-generate Tests – currently in the process of being released

Tools to validate and auto-generate safety evidence from high-level design models – in the process of transfer to UTRC

Tools to automatically analyze code for run-time errors – available and being used by UTRC, Boeing, Collins, FAA tech center and many others



TC3: V&V for Commercial Ops (Now ends FY22)

Impacts and Strategy – Heilmeyer Summary

Objective: Reduce the time required to certify state-of-the-art avionics capabilities for commercial transport.

Current state:

- The cost of validating, verifying, and certifying modern avionics systems is a barrier to deploying new systems.

New state in FY 20:

- Automated techniques reduce time for validation and verification evidence collection by 10-50% depending on the type of system.
- These techniques have been validated by industry partners and tools are released to and used by U.S. industry.
- A prototype for a new certification framework under consideration by the FAA.

Transformed NAS Enabling Capabilities for Design-Time Safety:

- Time to certification significantly reduced for both traditional and emerging markets
- Savings allow confidence from investors and greater competitiveness in emerging vehicle market

Approach: Automated tools developed by NASA are already being used by our industry and regulatory partners. Measure quantifiable impact of these capabilities through a combination of in-house (FAA partnership) and NRA partner assessments (proposals due July 2019). The NRA solicitation will be likely awarded in early FY 2020. We have already delivered draft documentation to the FAA for a new certification framework that may improve the end-to-end certification time.

System Wide Safety

TC3 Technical & Programmatic Progress Summary

There is an FAA-coordinated Overarching Properties Working Group to evaluate the benefit of and create a path forward for the NASA-developed Overarching Properties (OP).

First release of the Formal Requirements Elicitation Tool (FRET). Approximately 40% of all defects are created in the requirements phase (where they are the hardest to fix). The NASA-developed FRET tool provides a user-intuitive way for engineers to create correct requirements and the tests and monitors to assure those requirements.

System Wide Safety

TC3: Demonstrate requirement formalization

Motivation and Objective

Requirements engineering is a central step in the development of safety-critical systems. FRET supports a restricted natural language that enables the intuitive expression of requirements, while ensuring unambiguous semantics. The language is associated with formal semantics thus allowing the connection to formal analysis tools. FRET provides its users with explanations of the formal semantics in various forms: natural language, diagrams, interactive simulation. FRET is currently connected to the nuXMV and Cocosim analyzers for consistency analysis and verification of Simulink models, respectively.

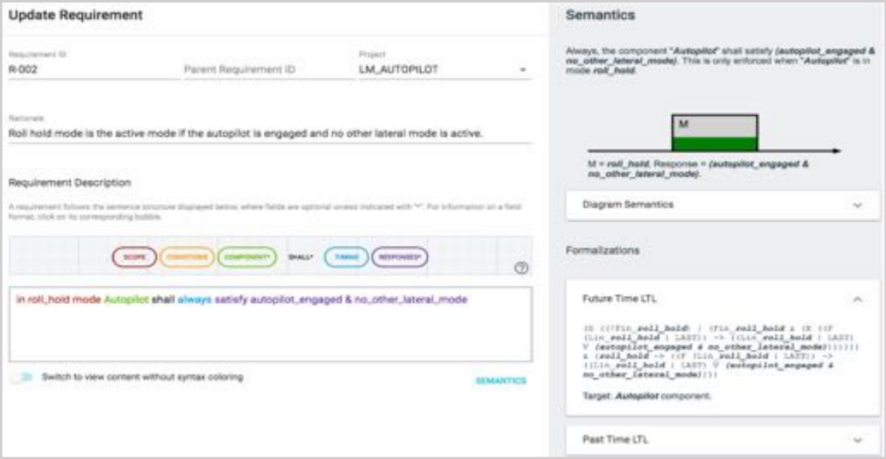
Milestone SWS.SAAFE-2.2:

- Demonstrate requirement formalization analysis and consistency

Approach

- Extensible grammar defines the language of FRET; requirements made up of fields for scope, conditions, component, timing, and responses.
- Compositional generation of semantics from requirement fields; semantics in future and past time metric temporal logic
- Options for understanding semantics, including interactive simulation
- Provide support for connecting requirement variables to model signals
- Extensive testing of semantics

(Next) Apply to missions; provide FRET support for correcting requirements



Update Requirement

Requirement ID: R-002

Parent Requirement ID

Project: LM_AUTOPILOT

Rationale: Roll hold mode is the active mode if the autopilot is engaged and no other lateral mode is active.

Requirement Description

A requirement follows the sentence structure displayed below, where fields are optional unless indicated with "*". For information on a field format, click on its corresponding bubble.

in roll_hold mode Autopilot shall always satisfy autopilot_engaged & no_other_lateral_mode

Switch to view content without syntax coloring

Semantics

Always, the component "*Autopilot*" shall satisfy *(autopilot_engaged & no_other_lateral_mode)*. This is only enforced when "*Autopilot*" is in mode *roll_hold*.

M = *roll_hold*, Response = *(autopilot_engaged & no_other_lateral_mode)*.

Formalizations

Future Time LTL

```
(G (((Fin_roll_hold) | (Fin_roll_hold & (X ((F
(Lin_roll_hold | LAST)) -> ((Lin_roll_hold | LAST)
V (autopilot_engaged & no_other_lateral_mode)))))))
& (roll_hold -> ((F (Lin_roll_hold | LAST)) ->
((Lin_roll_hold | LAST) V (autopilot_engaged &
no_other_lateral_mode)))))
```

Target: *Autopilot* component.

Accomplishment

- Supports milestone SWS.SAAFE-2.2 (Q2/FY19)
- First release of tool features intuitive user interface, semantics generation, interactive simulation, connection to analysis tools, requirements organization in databases, user manual
- Downloaded by on-site users; applied to formalize requirements

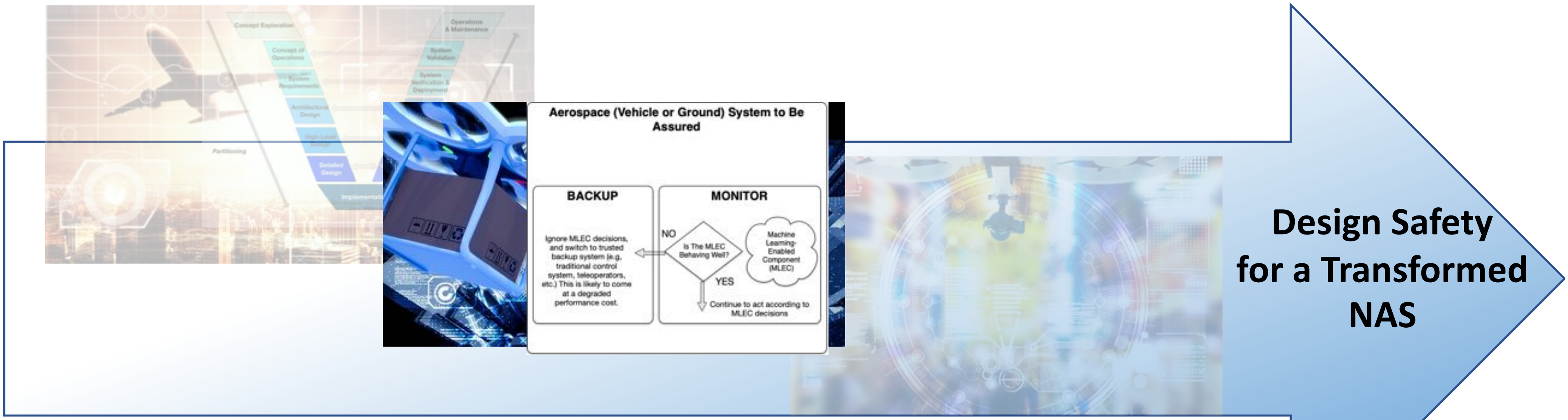
provided by: Lockheed Martin, Biosentinel, AVA, Boeing

- Three papers – 1 submitted, 2 to be submitted in the next month

System Wide Safety

Contributors: Giannakopoulou, Mavridou, Pressburger, Shi, Schumann (NASA ARC)

Design Time Safety Assurance



Aerospace (Vehicle or Ground) System to Be Assured

BACKUP

Ignore MLEC decisions, and switch to trusted backup system (e.g. traditional control system, teleoperators, etc.) This is likely to come at a degraded performance cost.

MONITOR

NO

Is The MLEC Behaving Well?

Machine Learning-Enabled Component (MLEC)

YES

Continue to act according to MLEC decisions

Design Safety for a Transformed NAS

TC3: Validation & Verification for Commercial Ops (Now-FY22)

TC4: Validation & Verification for Emerging Ops (Now-FY24)

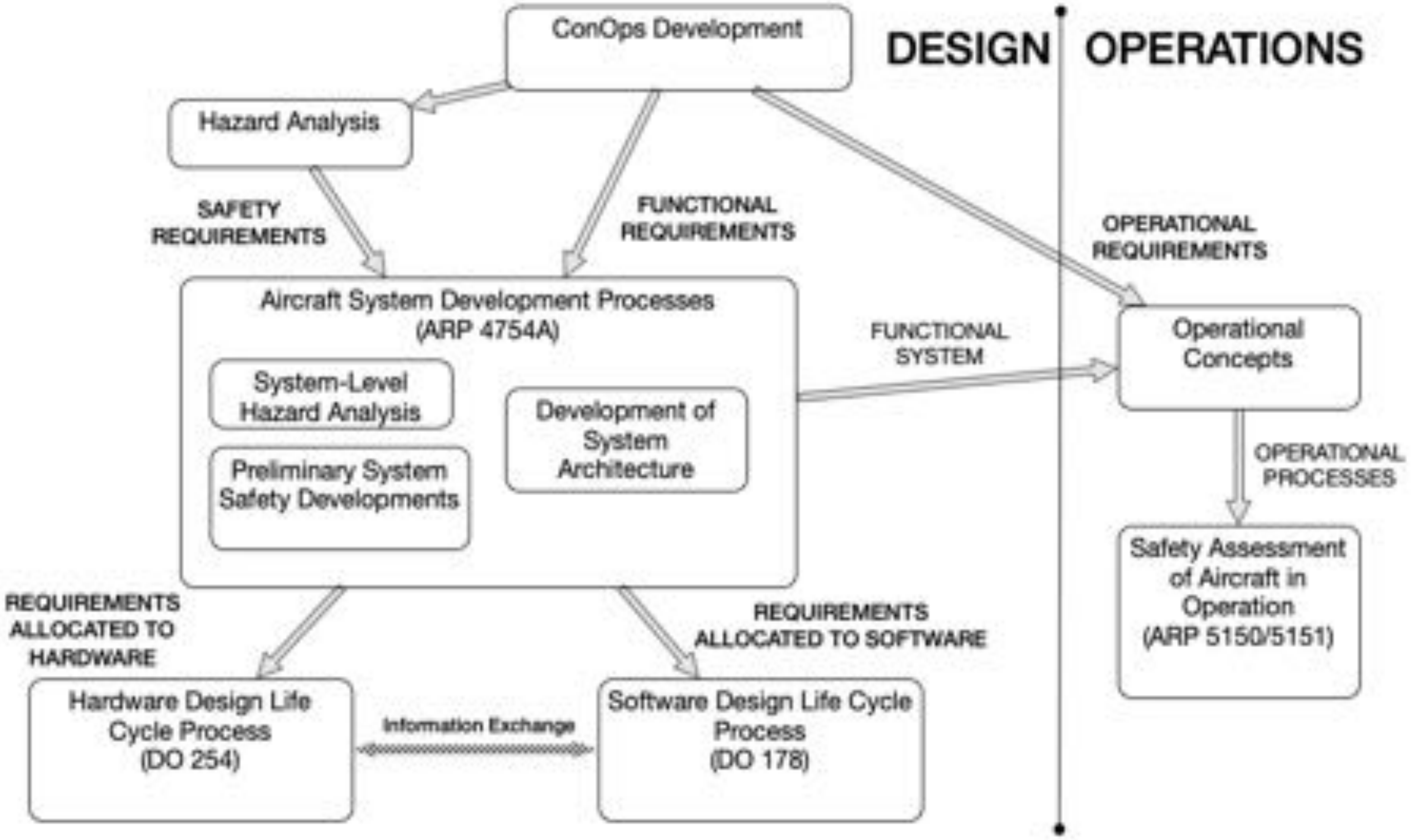
eTC5: Flexible Assurance for Systems-of-Systems Technologies (FY20-26)

TC4 will deliver recommendations to industry standards committees and to the regulators on the inclusion of machine-learning enabled components in highly-assured systems.

System Wide Safety

TC4: Complex Autonomous Systems Assurance (Now-FY24)

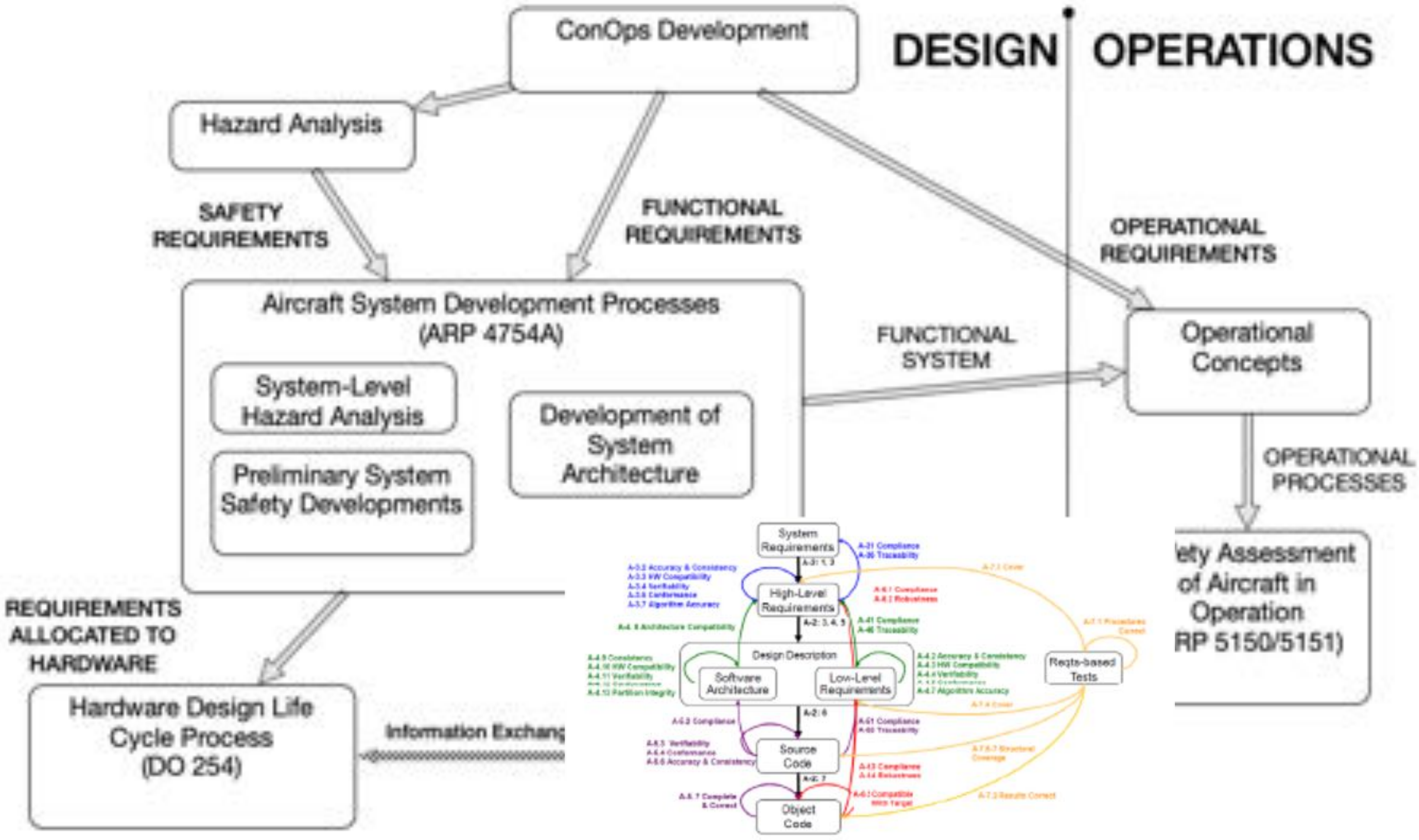
How We Assure Aerospace Systems Today


ConOps Development
DESIGN
OPERATIONS
Hazard Analysis
SAFETY REQUIREMENTS
FUNCTIONAL REQUIREMENTS
OPERATIONAL REQUIREMENTS
Aircraft System Development Processes (ARP 4754A)
System-Level Hazard Analysis
Preliminary System Safety Developments
Development of System Architecture
FUNCTIONAL SYSTEM
Operational Concepts
OPERATIONAL PROCESSES
Safety Assessment of Aircraft in Operation (ARP 5150/5151)
REQUIREMENTS ALLOCATED TO HARDWARE
REQUIREMENTS ALLOCATED TO SOFTWARE
Hardware Design Life Cycle Process (DO 254)
Information Exchange
Software Design Life Cycle Process (DO 178)

System Wide Safety

TC4: Complex Autonomous Systems Assurance (Now-FY24)

How We Assure Aerospace Systems Today

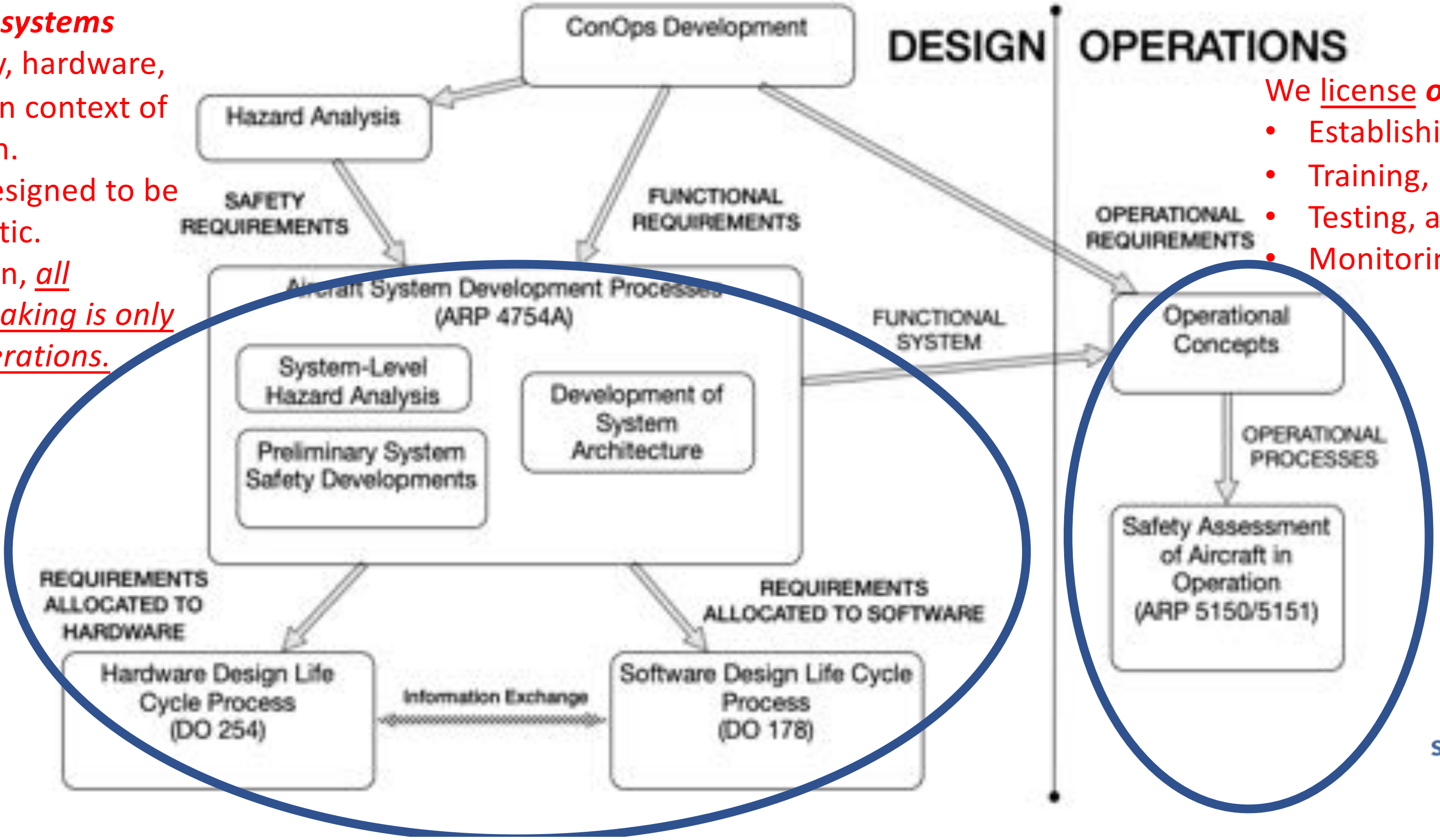


System Wide Safety

TC4: Complex Autonomous Systems Assurance (Now-FY24)

Keys to Assuring Aerospace Systems Today

- We certify ***systems*** (machinery, hardware, software) in context of the mission.
- Systems designed to be deterministic.
- After design, *all decision-making is only part of operations.*


ConOps Development
DESIGN
OPERATIONS
Hazard Analysis
SAFETY REQUIREMENTS
FUNCTIONAL REQUIREMENTS
OPERATIONAL REQUIREMENTS
Aircraft System Development Processes (ARP 4754A)
System-Level Hazard Analysis
Preliminary System Safety Developments
Development of System Architecture
FUNCTIONAL SYSTEM
Operational Concepts
OPERATIONAL PROCESSES
Safety Assessment of Aircraft in Operation (ARP 5150/5151)
REQUIREMENTS ALLOCATED TO HARDWARE
REQUIREMENTS ALLOCATED TO SOFTWARE
Hardware Design Life Cycle Process (DO 254)
Information Exchange
Software Design Life Cycle Process (DO 178)

We license ***operators*** by

- Establishing processes
- Training,
- Testing, and
- Monitoring

System Wide Safety

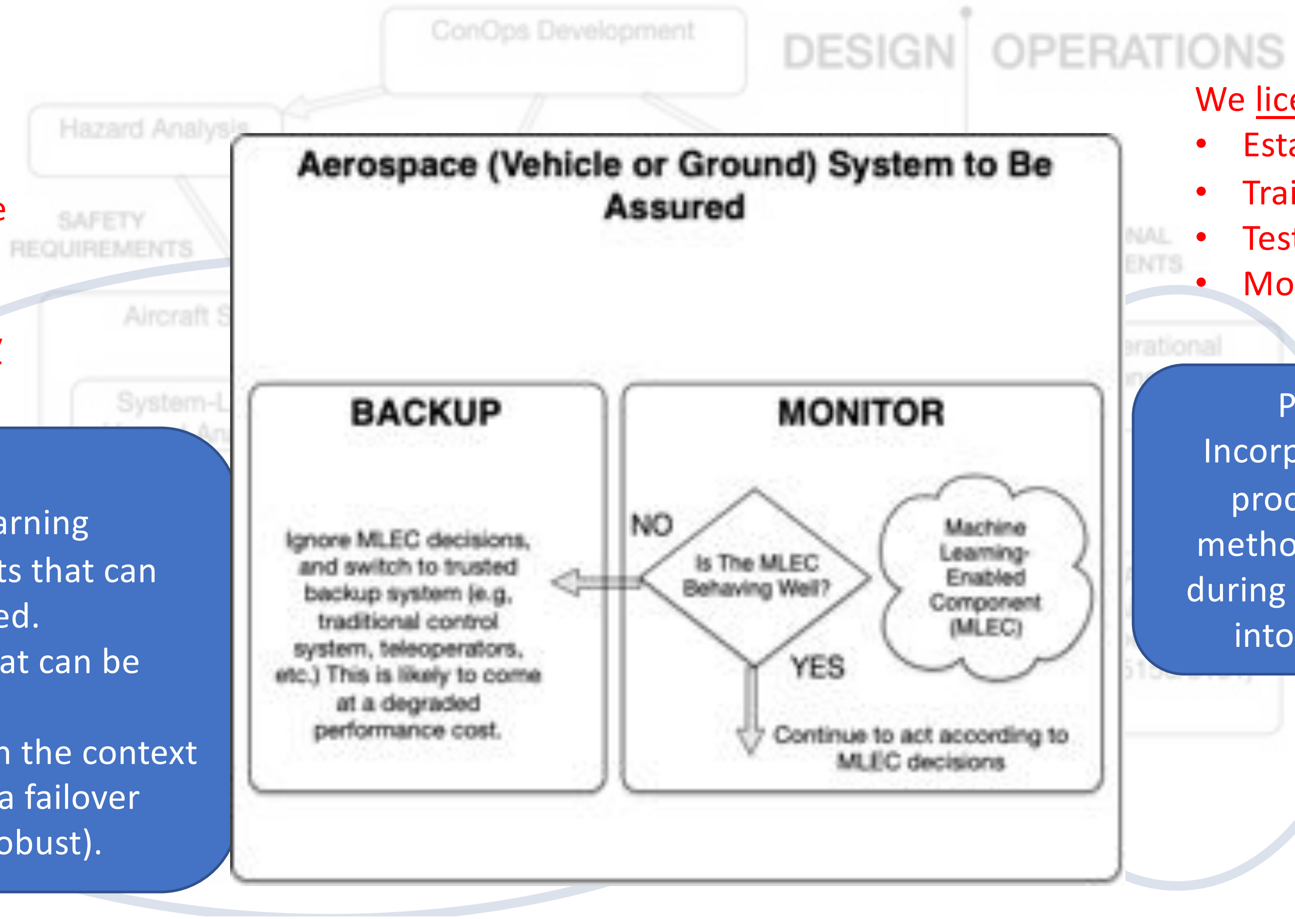
TC4: Complex Autonomous Systems Assurance (Now-FY24)

How to Assure Decision-Making at Design

- We certify ***systems*** (machinery, hardware, software) in context of the mission.
- Systems designed to be deterministic.
- After design, *all decision-making is only part of operations.*

Steps:

1. Choose machine-learning enabled components that can be bounded or tested.
2. Create a monitor that can be rigorously assured.
3. Certify the system in the context of the monitor and a failover plan/process (less robust).



ConOps Development
DESIGN
OPERATIONS
Hazard Analysis
SAFETY REQUIREMENTS
Aerospace (Vehicle or Ground) System to Be Assured
BACKUP
Ignore MLEC decisions, and switch to trusted backup system (e.g. traditional control system, teleoperators, etc.) This is likely to come at a degraded performance cost.
MONITOR
NO
Is The MLEC Behaving Well?
YES
Machine Learning-Enabled Component (MLEC)
Continue to act according to MLEC decisions

We license ***operators*** by

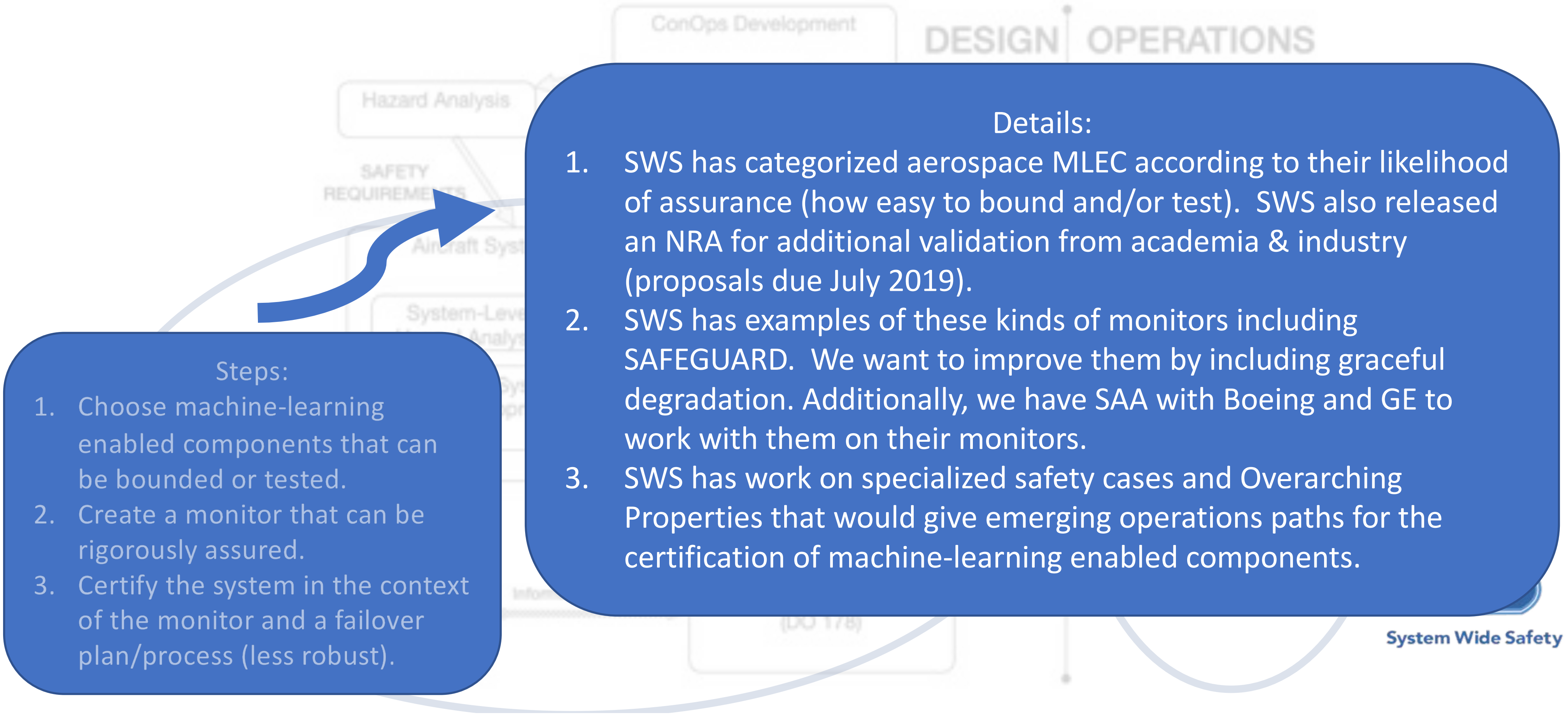
- Establishing processes
- Training,
- Testing, and
- Monitoring

PLAN:
Incorporate the processes & methods we use during operations into design.

System Wide Safety

TC4: Complex Autonomous Systems Assurance (Now-FY24)

Plan for Assuring Decision-Making Systems at Design



Steps:

1. Choose machine-learning enabled components that can be bounded or tested.
2. Create a monitor that can be rigorously assured.
3. Certify the system in the context of the monitor and a failover plan/process (less robust).

Details:

1. SWS has categorized aerospace MLEC according to their likelihood of assurance (how easy to bound and/or test). SWS also released an NRA for additional validation from academia & industry (proposals due July 2019).
2. SWS has examples of these kinds of monitors including SAFEGUARD. We want to improve them by including graceful degradation. Additionally, we have SAA with Boeing and GE to work with them on their monitors.
3. SWS has work on specialized safety cases and Overarching Properties that would give emerging operations paths for the certification of machine-learning enabled components.

TC4: Complex Autonomous Systems Assurance (Now-FY24)

Impacts and Strategy – Heilmeyer Summary

Objective: Develop a prototype certification process for autonomous aerospace systems that will be NASA's recommendation to the FAA, UAST, the Flight Safety Foundation and other standards committees.

Current state:

- Assurance of autonomous systems can't be accomplished in the framework of our current process.
- Certification depends upon a full exercise of possible behaviors, and
- The set of possible behaviors for autonomous systems is too large.

New state in FY 24: NASA will deliver a recommendation for the assurance of some machine-learning-enabled components within an overall autonomous systems architecture. This recommendation will include a process by which you can collect evidence for target levels of safety and risk.

Transformed NAS Enabling Capabilities for Design-Time Safety:

- Characterization of ML algorithm behaviors
- Bounding of 'safe' behaviors for some ML algorithms
- Assurance of monitors and safety-cases with failover plans

Approach: Build on NASA's leadership in assurance of autonomy (help and partnership requested by DARPA, AFRL, NIST, Johns Hopkins, Boeing, Nuro, etc.). Continue collaboration with academia and OGA on the analysis of machine-learning algorithm behaviors. Direct NASA's expertise on runtime monitoring and safety cases towards the bounding of autonomy and the assurance of contingency plans.

System Wide Safety

TC4 Partnership Progress

New agreements for the assurance of autonomy with AFRL, Boeing, and GE are complete.

DARPA has asked NASA to attend and act as an expert reviewer for its Assured Autonomy program.

New agreement with Nuro (autonomous car company operating in 4 cities) nearing completion. Continuing discussions with Google Loon and Wing.

NRA released 5/1 for industry and academic partners to help with autonomous systems assurance. Proposals are due mid-June.

System Wide Safety

TC4 Technical Progress Summary

- Completed milestone on the review of currently-used machine-learning algorithms and their assurability.

- One draft document on the OP delivered to the FAA September 2018. Another NASA TM in review now.

- Each of the following capabilities will feed into an overall assurance argument for the use of autonomous decision-making components within a safety-critical system:

    - Completed milestone on capability to explain machine-learning enabled components (including deep-learning neural networks).

    - Completed milestone on capability to ensure that machine-learning and optimization algorithms *as implemented in code* are provably correct.

TC4: Explainability for Autonomy Algorithms

Motivation and Objective

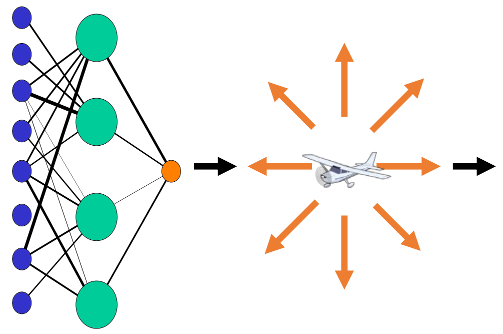
As autonomy becomes more complex, it also becomes more unpredictable, especially with the addition of machine learning. We seek to mitigate these issues with: 1) Explainable AI - explain decisions made by "black box" AI, 2) Justifiable trust in AI performance – verify that the AI system is performing as well as advertised

Milestone SWS.CASA-3.2:

- Develop and demonstrate basic capabilities for explanation of results produced by autonomy algorithms
- Exit criteria – Describe methods for explaining AI based control systems and for justifiable trust in AI performance. Methods include attribution analysis, rule conversion, distance metric analysis and transfer learning analysis.

Approach

- Convert black box system into explainable system including Bayesian rule lists, explainable trees and explanation templates
- Re-engineer black box system (e.g. replace top of deep neural net) to help analyze relation between decisions and training data.
- Analyze robustness of performance and confidence ratings on tests from original data distribution and transfers to new data distribution.



```
if conflict to left
    go up with probability .19
else if conflicts are above
    go left with probability .87
else
    go up with probability .07
…
...
...
```

Accomplishment

- Contributes to milestone SWS.CASA-3.2 (6/30/2019)
- Converted neural network control system to Bayesian Rule Lists, Grammar-based decision trees and Explanation templates
- Performed sensitivity analysis based on integrated gradients, and time-extended LSTMs to black box system.
- Created nearest-neighbor based explanation system allowing decisions from deep neural network to be traced back to training data.
- Publication (in review): "Challenges of Explaining Real-Time Planning," ICAPS, July 2019

Contributors: Agogino, Giannakopoulou, Lee (NASA ARC)

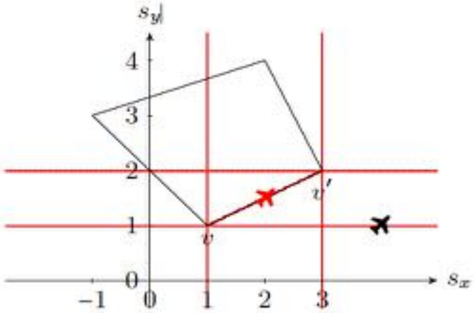
TC4: Mitigation of Numerical Errors

(Emerging Operations Design Assurance/Addressing Residual Risk in Autonomous Systems)

Motivation and Objective

Safety of autonomous operations depends on numerically intensive algorithms for problems such as geo-spatial containment, weather avoidance, and aircraft separation. This category of algorithms has potential for incorrect safety-critical decisions resulting from floating-point round-off errors.

The objective is to develop a capability to ensure that floating-point implementations make the same correct critical decisions as algorithms formally verified assuming infinitely precise computations on real numbers



Example points of potential incorrect decisions

Approach

- Combine capabilities of three formal analysis tools to create a new capability to ensure that a C implementation of a formally specified algorithm implements the same critical decisions. The process is to automatically transform a verified real-number specification of an algorithm to a generated software implementation with proven verification conditions.
- Building Blocks:
  - Algorithms verified using PVS theorem proving systems (https://github.com/nasa/PolyCARP)
  - PRECiSA static analysis tool (https://github.com/nasa/PRECiSA), and
  - FRAMA-C static analyzer (https://frama-c.com/)

Accomplishment

- Developed and demonstrated capability to find and correct critical software defects introduced by floating-point roundoff error
- Completion of milestone CASA 5.1
  - *Provably Correct Floating-Point Implementation of a Point-in-Polygon Algorithm, by Moscato, Titolo, Feliu, and Munoz; to appear in FM2019: 3rd World Congress on Formal Methods, October 2019*

System Wide Safety

POC: Cesar Munoz

TC4: Overarching Properties

(Commercial Operations Design Assurance/Streamlining Assurance)

Motivation and Objective

Current assurance of software-intensive systems for commercial aviation relies on a collection of industry-consensus standards such as RTCA DO-178C, SAE ARP 4754A, and ARP 4761. There are increasing concerns that these standards may not be sufficient for anticipated future systems.

The objective is to develop a technology-independent approach to enable effective assurance and approval for both current and future software-intensive aerospace systems

Approach

- Collaboration with FAA and Industry (initiated under IA1-1407 Annex 7 *Streamlining Assurance Processes;* new agreement pending)-- develop and validate *Overarching Properties (OP)*
- Develop sequence of increasingly complex worked examples to provide guidance
- Assess whether OP provide a viable alternative to DO-178C and related guidance documents
- Continue in a leading role in the FAA-coordinated Overarching Properties Working Group

Overarching Properties (as of 2019-04-11)

Intent: The *defined intended behavior* is correct and complete with respect to the *desired behavior.*

Correctness: The *implementation* is correct with respect to the *defined intended behavior,* under *foreseeable operating conditions.*

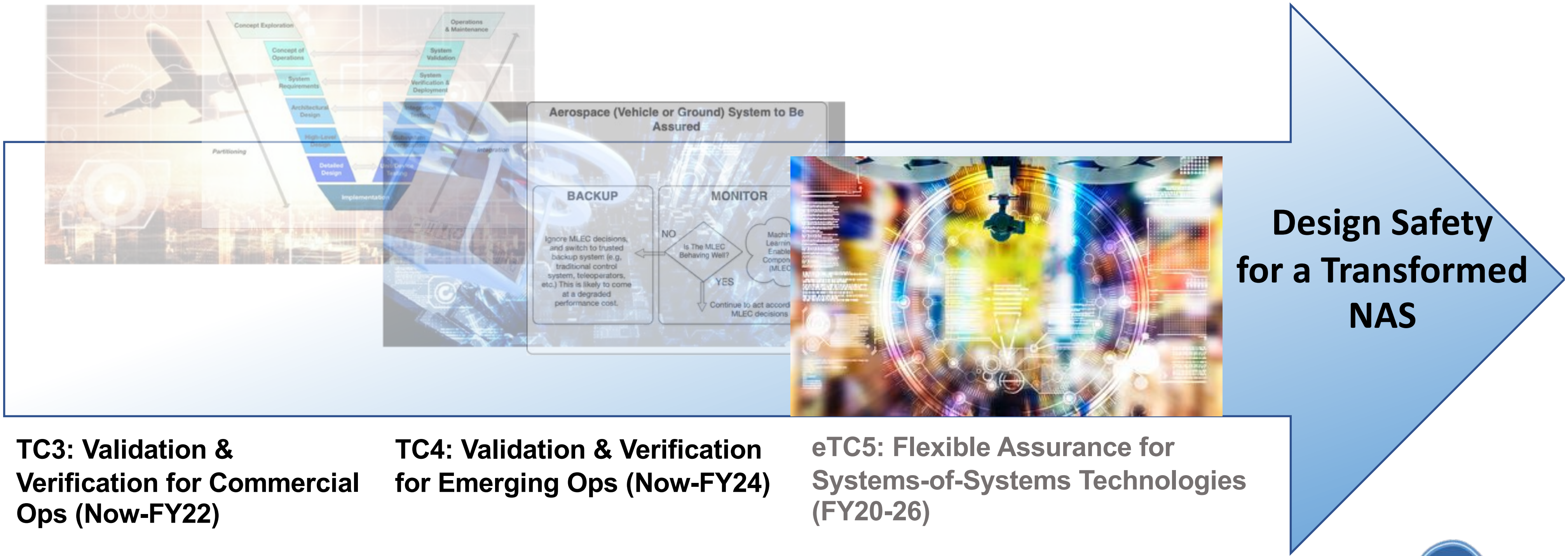
Innocuity : Any part of the *implementation* that is not required by the *defined intended behavior* has no *unacceptable safety impact.*

Accomplishment

- Completed milestone SAAFE 7.1 – *Develop and deliver draft guidance for demonstrating justifiable confidence in safety claims based on showing satisfaction of Overarching Properties (crawl)*
  - 2018 September: Delivered draft document to FAA -- *Understanding Overarching Properties: First Steps,* (author: C. Michael Holloway)
  - Developed draft NASA TM *Retrospectively Documenting Satisfaction of the Overarching Properties: An Exploratory Prototype,* by Mallory S. Graydon and Jared D. Cronin (in review)
- Significant contributions and presentations to Overarching Properties Working Group

POC: Michael Holloway

Design Time Safety Assurance



Design Safety for a Transformed NAS

TC3: Validation & Verification for Commercial Ops (Now-FY22)

TC4: Validation & Verification for Emerging Ops (Now-FY24)

eTC5: Flexible Assurance for Systems-of-Systems Technologies (FY20-26)

eTC5 is under development now. Our plan is to work with other government agencies (USGS, AFRL) to develop challenges that let us understand better the gaps we have for rapid, flexible assurance of interacting systems.

System Wide Safety

Executive Summary
eTC5: Flexible Assurance for Systems-of-Systems Technologies (FASST)

Challenge Objective: Develop, demonstrate and validate a process that allows us to assure system-level safety in a future aerospace system with heterogeneous and rapidly-changing decision-making components (vehicles, third-party service providers, etc.).

Focus

- Highly interconnected and heterogeneous systems, such as those enabled by UTM, are prone to emergent behaviors and to exploitation by selfish participants.

- Current system safety assurance assumes rational and cooperative behavior. However, as the cost for entry into the aviation market goes down, we need additional safeguards for decision-making that is either incompetent or adversarial, or to detect behavior that is rational at the vehicle level, but harmful at the airspace system level.

Why This Work is Prioritized

Achieving UAM at scale within the short time-frame predicted while maintaining acceptable societal risk will require minimum design re-work, especially if the U.S. is to maintain a competitive advantage.

System Wide Safety

Backup

System Wide Safety

Thrust 5 - NASA's Vision for Operational Safety to 2045

Domain Specific (In-time) Safety Monitoring and Altering Tools (2015-2025)

Expanded system awareness through increased access to safety relevant data and initial integration of analysis capabilities; improved safety through initial real-time detection and alerting of hazards at the domain level and decision support for limited, simple operations.

Integrated Predictive Technologies with Domain Level Application (2025-2035)

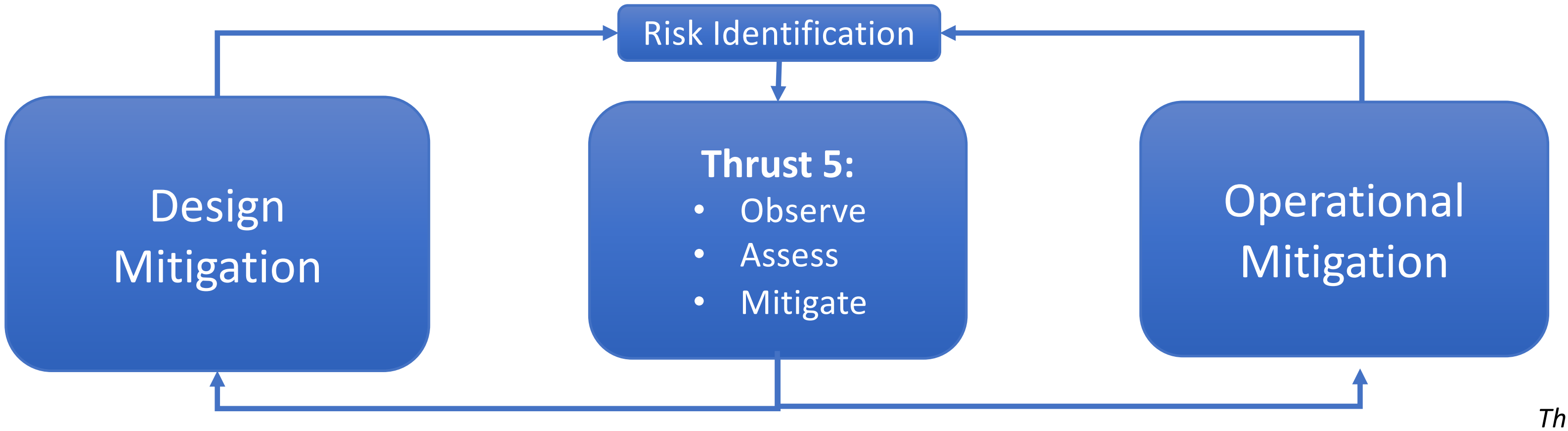
NAS-wide availability of more fully integrated in-time detection and alerting for enhanced risk assessment and support of initial assured human and machine decision support for mitigation response selection for more complex operations.

Adaptive Real-time Safety Threat Management (2035-2045)

Fully integrated threat detection and assessment that support trusted methods for dynamic, multi-agent planning, evaluation, and execution of in-time risk mitigating response to hazardous events.

System Wide Safety

System-Wide Safety and Thrust 5



Risk Identification

Design Mitigation

Thrust 5:
- Observe
- Assess
- Mitigate

Operational Mitigation

This loop:
months to years
years to decades

This loop:
Seconds to hours
Hours to days

Sub-Projects

Verification & Validation of Flight Critical Systems

In-time System-wide Safety

System Wide Safety

TC2: In-Flight Safety Predictions for Emerging Operations

Challenge Objective: Demonstrate a data-driven safety assurance capability that provides a timely assessment, prediction, and mitigation of safety risks for UAS urban operations.

Focus

- TC2 focuses on demonstration of the Thrust 5 In-Time System-Wide Safety Assurance (ISSA) capability as applied to safety-critical risks for low-altitude urban UAS operations. Planned demonstration within UTM TCL4 this year. TC2 was already well-aligned with UAM.
- Changed the TC2 technical plan to direct future TC2 work from UAS towards UAM with sUAS used as a surrogate when larger passenger- or cargo-carrying vehicles cannot be used for assessment or demonstration.
- FY20-FY22 efforts contain:
  - An RFP for emerging operations partnerships.
  - Data-driven safety assessments with UAST, and academia.
  - Models and metrics to characterize safe operations, and assurance tools for predictive system components.
  - System evaluations.
- This work as planned is already well-aligned with UAM. FY19 augmentation is directed toward integrating the ISSA capability into ATM-X to accelerate incorporation into Grand Challenge demonstration. This work will continue into FY20
- FY21 and 22 resources are shifted to TC6 for development of the In-Time Aviation Safety Management System (IASMS) as called for in the NRC Thrust 5 report.

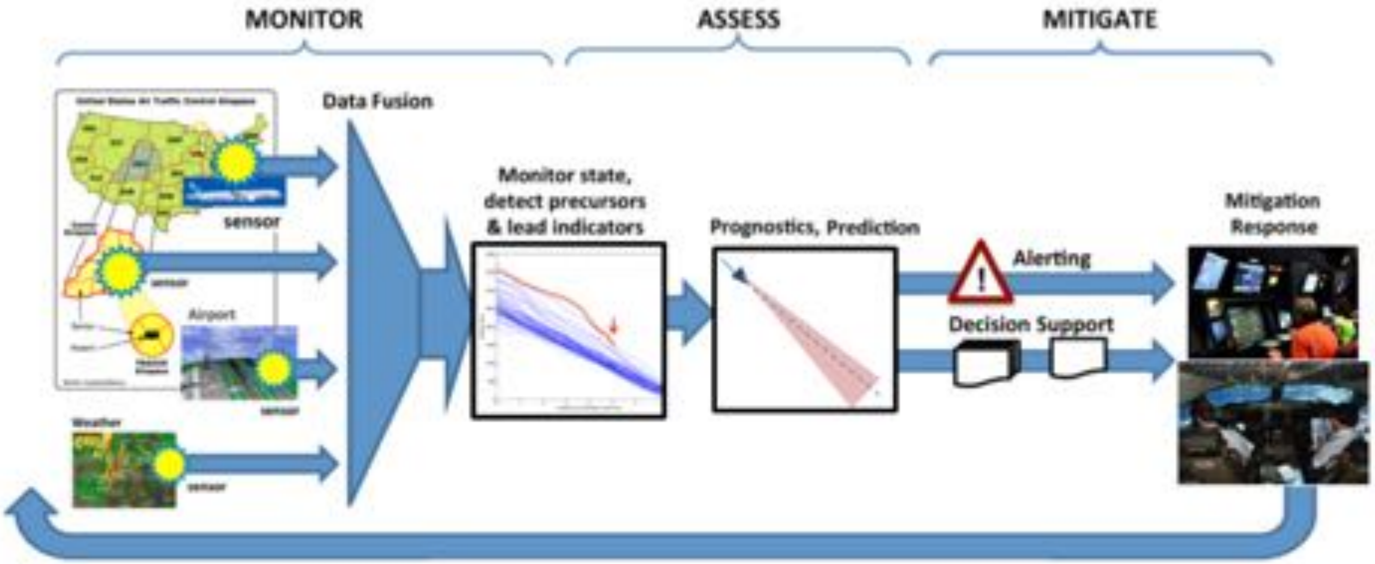
Why This Work is Prioritized

UAM operations are significantly different from standard operations in ways that will make our current operational safety procedures and processes obsolete. Maintaining and/or improving safety in this new operational paradigm will require stronger proactive and novel predictive capabilities. Continuing with current operational safety processes and procedures will delay the growth of the market. Eliminating current operational safety processes and procedures with no replacement carries unacceptable societal risk.

System Wide Safety

SWS Overview

Objectives

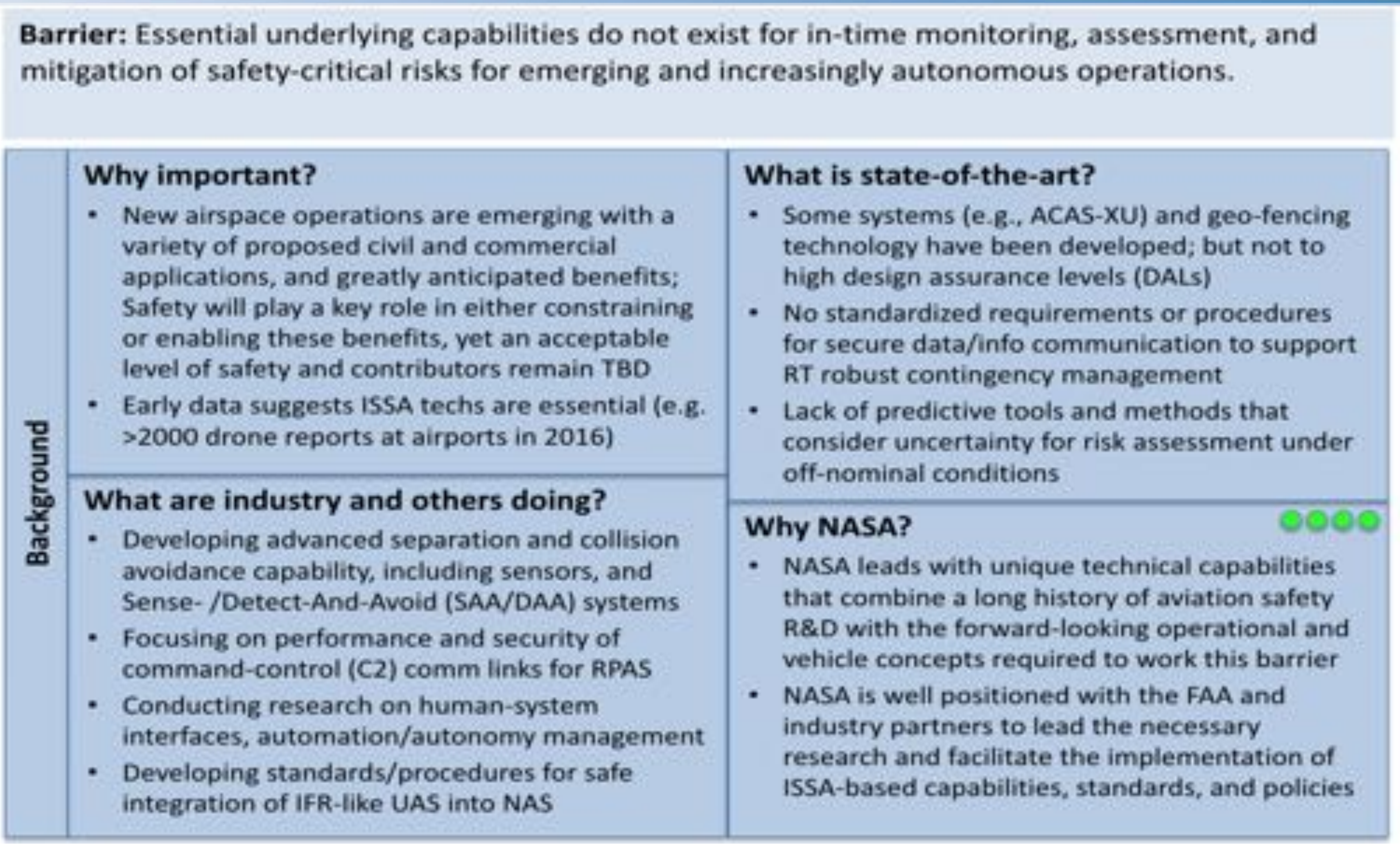


Feedback loop:

- More selective monitoring
- Improved models for assessment
- Evaluation and validation of mitigation strategies
- Supports existing off-line safety assurance methods

30-yr roadmap →

TC2 (Emerging Ops) Overview



Barrier: Essential underlying capabilities do not exist for in-time monitoring, assessment, and mitigation of safety-critical risks for emerging and increasingly autonomous operations.

Background

Why important?

- New airspace operations are emerging with a variety of proposed civil and commercial applications, and greatly anticipated benefits; Safety will play a key role in either constraining or enabling these benefits, yet an acceptable level of safety and contributors remain TBD
- Early data suggests ISSA techs are essential (e.g. >2000 drone reports at airports in 2016)

What are industry and others doing?

- Developing advanced separation and collision avoidance capability, including sensors, and Sense- /Detect-And-Avoid (SAA/DAA) systems
- Focusing on performance and security of command-control (C2) comm links for RPAS
- Conducting research on human-system interfaces, automation/autonomy management
- Developing standards/procedures for safe integration of IFR-like UAS into NAS

What is state-of-the-art?

- Some systems (e.g., ACAS-XU) and geo-fencing technology have been developed; but not to high design assurance levels (DALs)
- No standardized requirements or procedures for secure data/info communication to support RT robust contingency management
- Lack of predictive tools and methods that consider uncertainty for risk assessment under off-nominal conditions

Why NASA? ●●●●

- NASA leads with unique technical capabilities that combine a long history of aviation safety R&D with the forward-looking operational and vehicle concepts required to work this barrier
- NASA is well positioned with the FAA and industry partners to lead the necessary research and facilitate the implementation of ISSA-based capabilities, standards, and policies

ystem Wide Safety

ISSA –TC2 Domain Space & Research Scope

TC2 Statement: Develop and demonstrate a data-driven capability to assess, predict, and mitigate risks during highly-autonomous urban flight operations.

Key Attributes:

Initially targets **5 safety risks** identified by UTM and others*****:**

1) flight outside of approved airspace
2) unsafe proximity to people or property
3) critical system failure (loss of link, loss or degraded GPS, loss of power, engine failure)
4) loss-of-control**
5) cyber-security related risks

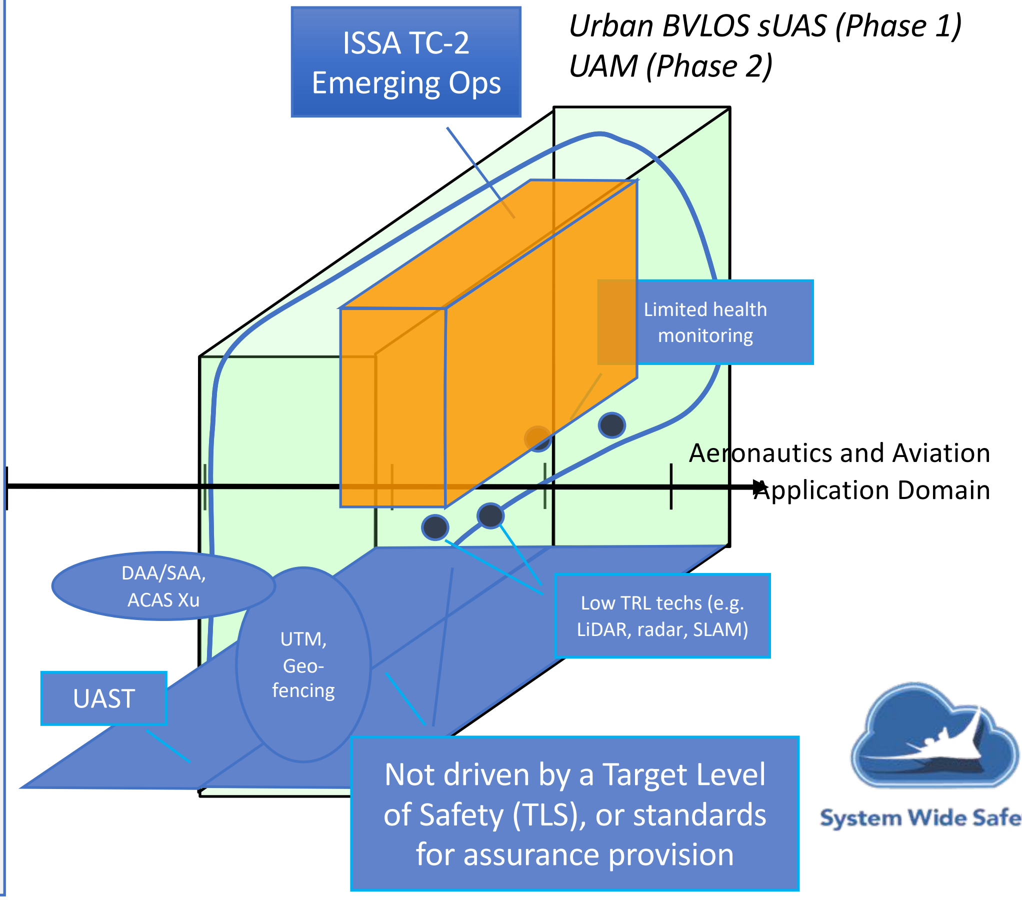
Assumes air traffic risks addressed by others (UTM, UAS in NAS, ATM-X)

2 Phases to align w ARMD guidance

Key Collaborators:

- **UTM/ATM-X** regarding ISSA info services and models to mitigate targeted risks; and for data collection/test opportunities
- **UAS operators and manufacturers** regarding automated mitigations, joint demos, and tech transfer paths
- **UAST** for alignment with identified risks and transferring findings and Safety Enhancements to **FAA/industry**

*(e.g., UAST, JARUS, ASTM)


ISSA TC-2
Emerging Ops
Urban BVLOS sUAS (Phase 1)
UAM (Phase 2)
Limited health monitoring
Aeronautics and Aviation Application Domain
DAA/SAA, ACAS Xu
UTM, Geo-fencing
UAST
Low TRL techs (e.g. LiDAR, radar, SLAM)

Not driven by a Target Level of Safety (TLS), or standards for assurance provision

System Wide Safety

ISSA TC2 Progress

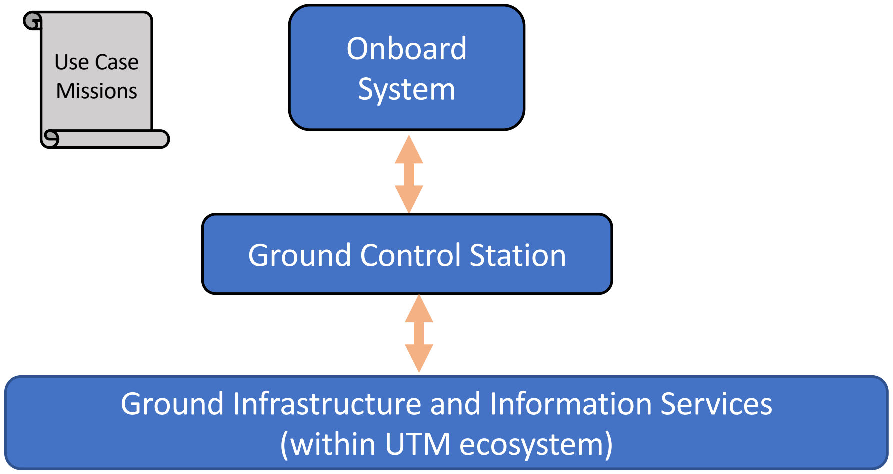
Develop Baseline Testing Capability

Milestone: Baseline capability testing

Objectives:

(1)Test and evaluate baseline architecture and selected functional elements

(2)Collect data to support future development of envisioned capabilities



Use Case Missions

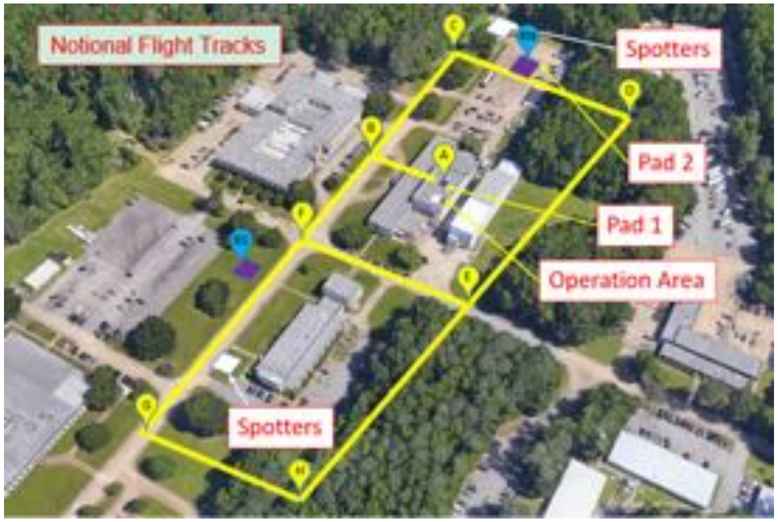
Onboard System

Ground Control Station

Ground Infrastructure and Information Services (within UTM ecosystem)

Other Drivers:

- Confirm consistency and interaction with UTM infrastructure
- Integrate relevant recent research
- Begin spiral RDT&E process
- Requirements discovery



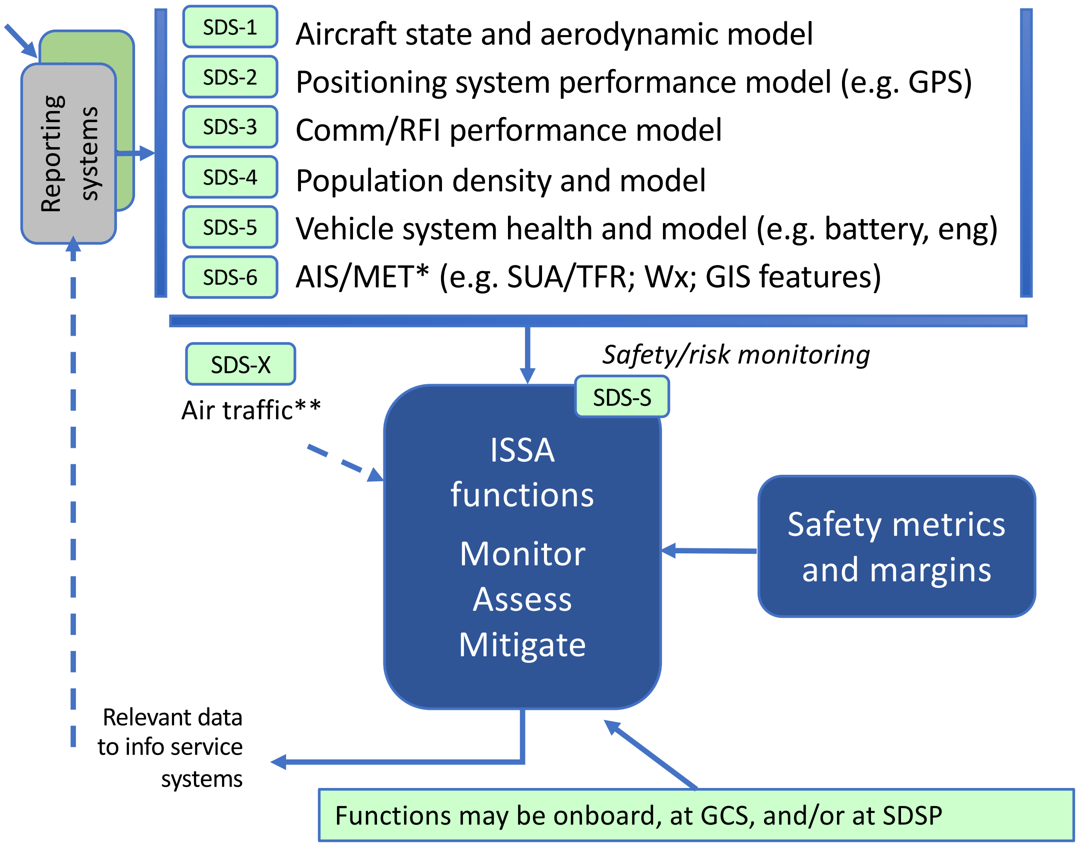
Within CERTAIN Test Range

System Wide Safety

ISSA TC2 Progress

Establish EO Functions and Reference Architecture

Model-based predictive capabilities



Reporting systems

SDS-1	Aircraft state and aerodynamic model
SDS-2	Positioning system performance model (e.g. GPS)
SDS-3	Comm/RFI performance model
SDS-4	Population density and model
SDS-5	Vehicle system health and model (e.g. battery, eng)
SDS-6	AIS/MET* (e.g. SUA/TFR; Wx; GIS features)

SDS-X

Air traffic**

Safety/risk monitoring

SDS-S

ISSA functions

Monitor

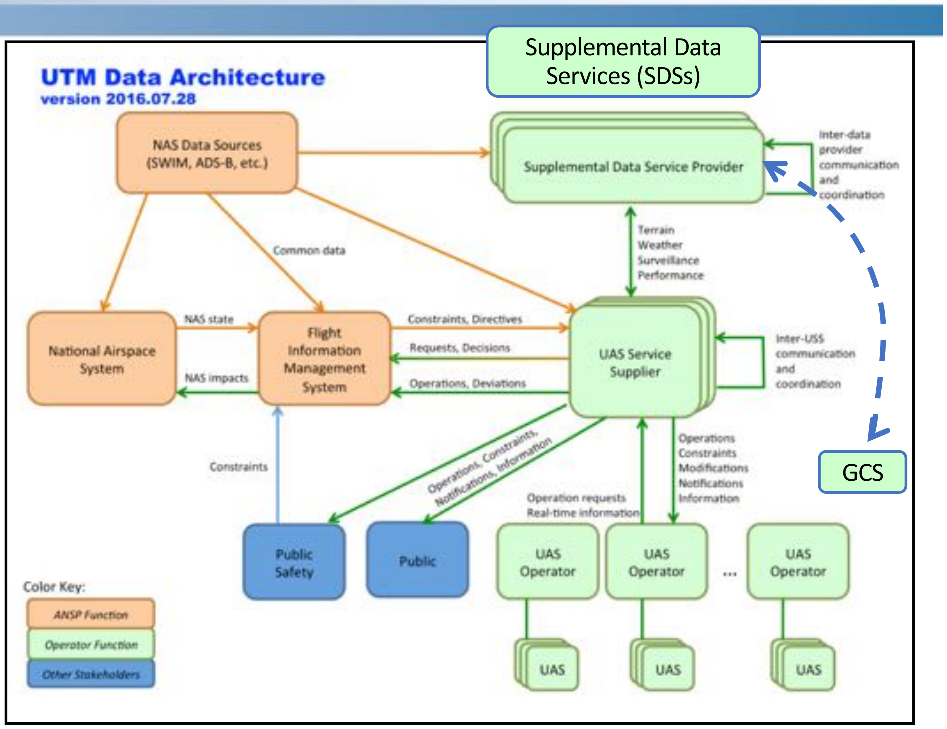
Assess

Mitigate

Safety metrics and margins

Relevant data to info service systems

Functions may be onboard, at GCS, and/or at SDSP



Supplemental Data Services (SDSs)

GCS

*TC-2 R&D assumes that some AIS/MET services already exist, or are in development by others

**TC-2 R&D assumes air traffic-related services are addressed by others (e.g. UTM, ACAS-XU) (but TC2 construct must be consistent with these solutions and interoperable)

“Mature” SWS Services

Non-Participant Casualty Risk Assessment

Intended function: Estimate, track, and predict risk of impacting populated areas in the event of critical system failure or loss-of-control; Can be executed pre-flight using flight plan or in-flight on cFS

Outputs: Casualty and LOC probabilities, Likelihood & Severity values, Recommended course of action (abort, land, RTL, continue)

Inputs: (see next chart)

Recent testing: UTM TCL-3/4 sim and flight tests (2018, 2019)

Battery Prognostics

Intended function: Estimate, track, and predict state-of-charge and remaining useful life of onboard power source(s)

Outputs: Estimated time when end of discharge (EOD) will be reached (or est. remaining flight time); Probability of reaching EOD before end of mission

Inputs: (see next chart)

Recent testing: UTM TCL-4 Sprint sims (2019); SWS flights (2018, 2019)

Proximity to Obstacles*

Intended function: Estimate, track, and predict proximity (time and distance) to fixed vertical structures near the flight path

Outputs: Portions of vehicle trajectory that violate proximity thresholds (incl. start/end pts); Nearest approach point; Distance to nearest approach point; Severity of violation (see note)

Inputs: (see next chart)

Recent testing: UTM TCL-4 Sprint sims (2019); SWS flights (2018)

*1st step toward a more general service/function: “Proximity to Loss of Safety Margin”

Future plan (under SWS): Advancing TRL and refining requirements through series of test/evaluate cycles,

1) Integration across metric trackers for aggregate safety anomaly, trend, and precursor detection capabilities
2) On-board real-time versions for tactical assessment and input to auto-contingency selection and execution functions
3) Application of assurance methods for safety-critical elements

Input Data Requirements

Pre-flight

Info type	Source	NPCRA	BP	PtO	Comment
Configuration settings	SWS	X	X	X	SWS researchers will provide config files
Aircraft specifications	?	X	X	X	Size, weight, model, #rotors/engine, etc. (Can be via GUI)
Aerodynamic model	?	X	X	X	Level-of-detail TBD (e.g. aero coefficients)
Flight plan	Testbed?	X	X	X	4D preferred (can be Mission Planner waypoint file)
Battery model	?		X		Calibration procedure req'd (re-cal after 8-10 flights)
3D geo-feature database	Testbed?	X		X	Buildings/obstacles (GIS model preferred)
Population density database	SWS	X		X	Stored at the server; 3rd party vendor; 2-3 wks lead time
Wind vector or model	Testbed?	X		X	If a static vector, can be input as part of config settings
USS/Testbed/SWIM info		-	-	-	SWS would like to log this to support its future work

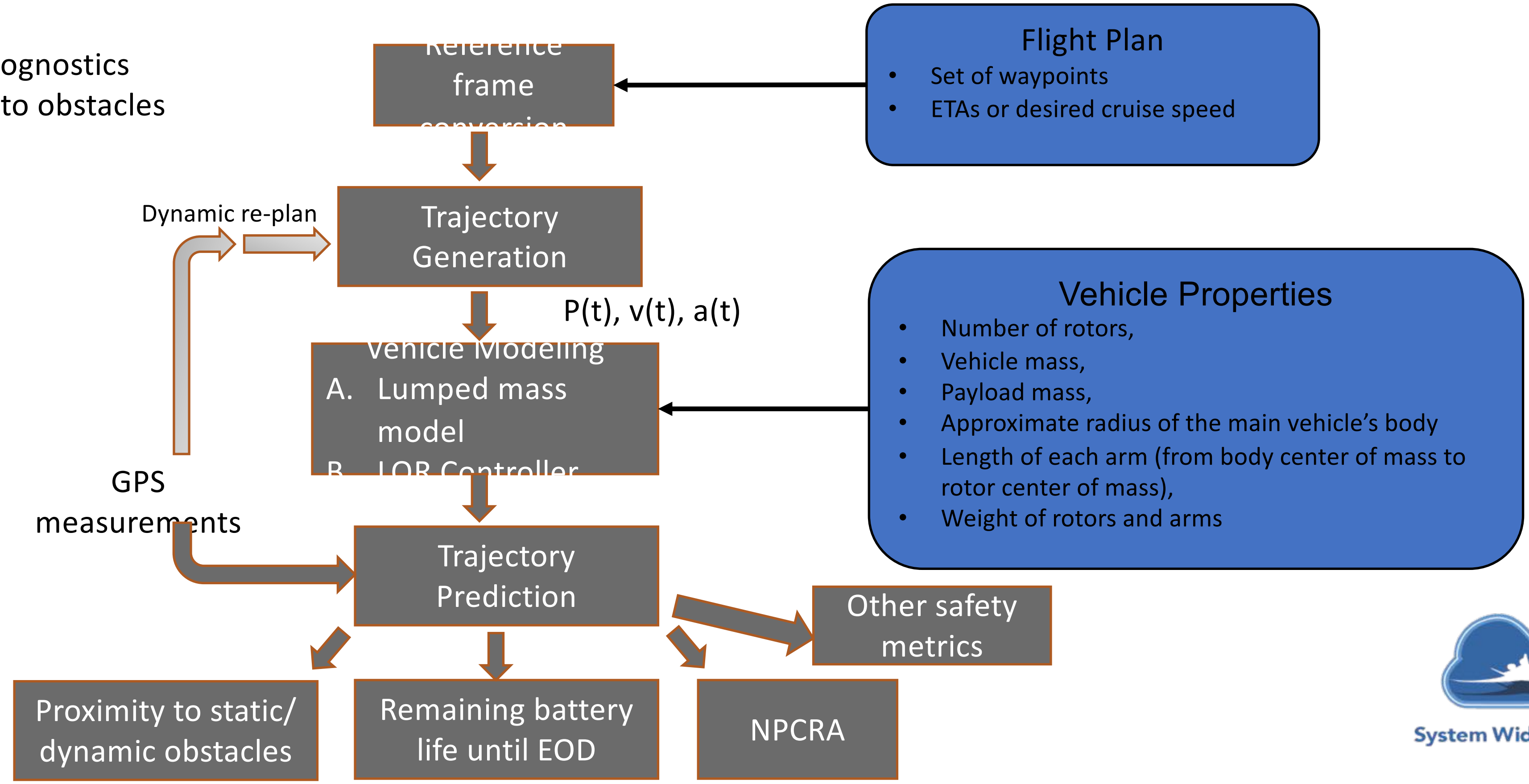
In-flight
(@ 1 Hz or greater)

Source could be Testbed, USS, GCS, or aircraft

Info type	NPCRA	BP	PtO	Comment
Aircraft state (position, velocity, etc)	X	X	X	
Battery state (voltage, current, temp, …)	X	X		For each on-board battery pack
Engine/motor state (current, temp, …)	X			
A/P state (auto, manual, land, RTL, etc)	X			
Nav system state (e.g. GPS SVs, DOPs, etc)	X			
Comm system state (e.g. RSSI)	X			
USS/Testbed/SWIM info	-	-	-	See above

TC2 UAS Services Schematic

Battery prognostics
Proximity to obstacles



Reference frame conversion

Flight Plan
- Set of waypoints
- ETAs or desired cruise speed

Dynamic re-plan

Trajectory Generation

P(t), v(t), a(t)

Vehicle Modeling
A. Lumped mass model
B. LQR Controller

Vehicle Properties
- Number of rotors,
- Vehicle mass,
- Payload mass,
- Approximate radius of the main vehicle's body
- Length of each arm (from body center of mass to rotor center of mass),
- Weight of rotors and arms

GPS measurements

Trajectory Prediction

Other safety metrics

Proximity to static/ dynamic obstacles

Remaining battery life until EOD

NPCRA

System Wide Safety

Collaboration Areas

- TC2: APT, Nexus
  - Models
    - Battery & aerodynamics
    - GNC models: GPS, control architecture, IMU,
    - Any sensors that could become the standard e.g. vibration sensors for motors?
    - Lessons learned from moving from APT 20 to APT 70 & APT 400? Important considerations?
    - Communication link issues? Frequency bands for operations
    - Operator architecture
  - Decision making capabilities? Any prognosticator in the loop
  - How do their vehicles compare to current developments for UAM? Is there a known standard?
  - Other than VTOL, any fixed-wing or hybrid configurations? For our model development.
  - Known issues - vehicle, infrastructure, GCS – future safety metric development
  - Challenges with airspace integration not necessarily vehicle centric
  - Certification or minimum safety requirements for flight from FAA/regulatory body etc?
  - RFI, GPS, GRASP(pre-flight or onboard CFS)
  - Flights? Where? Frequency? Duration? How autonomous? How many people for remote piloting?
  - Low altitude, higher resolution wind estimation and forecasting
  - What would they like to see? What do they need help with?

System Wide Safety