National Aeronautics
and Space Administration

AAM Ecosystem Working Group (AEWG) Aircraft Working Group

Expected Safety Level For AAM

100th Meeting of the AEWGs!

Oct 27, 2022

3:00 PM – 4:30 PM ET /

Today's Agenda

October 27, 2022			
Time (ET)	**Topic**	**Speaker**	**Location**
Time (EDT)	**Topic**	**Speaker**	Microsoft Teams Conferences IO [Conferences IO Link Here]
3:00 - 3:10PM	**Welcome and Logistics**	Carl Russell, NASA Wes Ryan, NASA	
3:20-3:30PM	**100th AEWG Meeting Celebration**	Davis Hackenberg, NASA	
3:20-3:30PM	**Opening Thoughts and Polling**	Wes Ryan, NASA	
3:20-4:00PM	**Panel Discussion**	Natasha Neogi, NASA Langley Kim Wasson, Joby Lowell Foster, Wisk Loyd Hood, University of Tulsa Kevin Rodgers, Northrop Grumman	
4:00-4:25PM	**Polling and Discussion**	Wes Ryan, NASA	
4:25 – 4:30PM	**Wrap-up**	Carl Russell, NASA	
FAA Disclaimer: *FAA participation in NASA forums and AAM community/stakeholder programs does not constitute FAA approval or endorsement*			

Logistics

- **AEWG Session** *(3:00PM – 4:30PM ET / 12:00AM – 1:130PM PT)*
  - **Q&A:** Conferences.io
    - Enter https://arc.cnf.io/sessions/cc22/#!/dashboardinto your browser
    - Questions will be addressed *if times permits or at the facilitator's discretion*
  - **Platform:** MS Teams
    - To access the individual breakout rooms, use the MS Teams meeting links in the agenda
    - The agenda is accessible at the following URL: https://nari.arc.nasa.gov/aewg-w-agenda
  - **Q&A:** MS Teams microphone, chat, and "Raise your hand" functions
    - Leave your cameras/webcams off to preserve WiFi bandwidth
    - Use your mute/unmute button (e.g. remain on mute unless you are speaking)
    - Enter comments/questions in the chat
    - Click the "Raise your hand" button if you wish to speak
    - Say your name and affiliation before you begin speaking

Purpose and Goals: Open Discussion

- **How do we define/measure safety?**
  - Design Safety and Operational Safety – Are they the same?
    - Can we Address Operational Safety by Design?
    - Can we Address Design Safety by Operational Limitations?

- **What SRM Tools are the ”Right” Tools to Properly Analyze Risk For New/Novel Aircraft and Operating Concepts?**
  - Are Traditionally Accepted Tools/Methods Applicable?
  - Should we Measure Safety per Flight, Per Flight Hour, etc.?

- **We all agree we can’t erode our current civil aviation safety expectations, but <u>how do we define those for each new operation</u>?**
  - Can’t use a singular approach or stack conservative estimates on top of each other. = what-if the good ideas into delayed release or death

Poll #1 – Safety Motivations

- What is the largest driver for AAM safety expectations?
  - Public Perception/Public Safety
  - Reliability/Resilience of Technology
  - Regulatory Expectations
  - Other?

Panel Discussion

Natasha Neogi, NASA Langley

Kim Wasson, Joby

Lowell Foster, Wisk

Loyd Hood, University of Tulsa

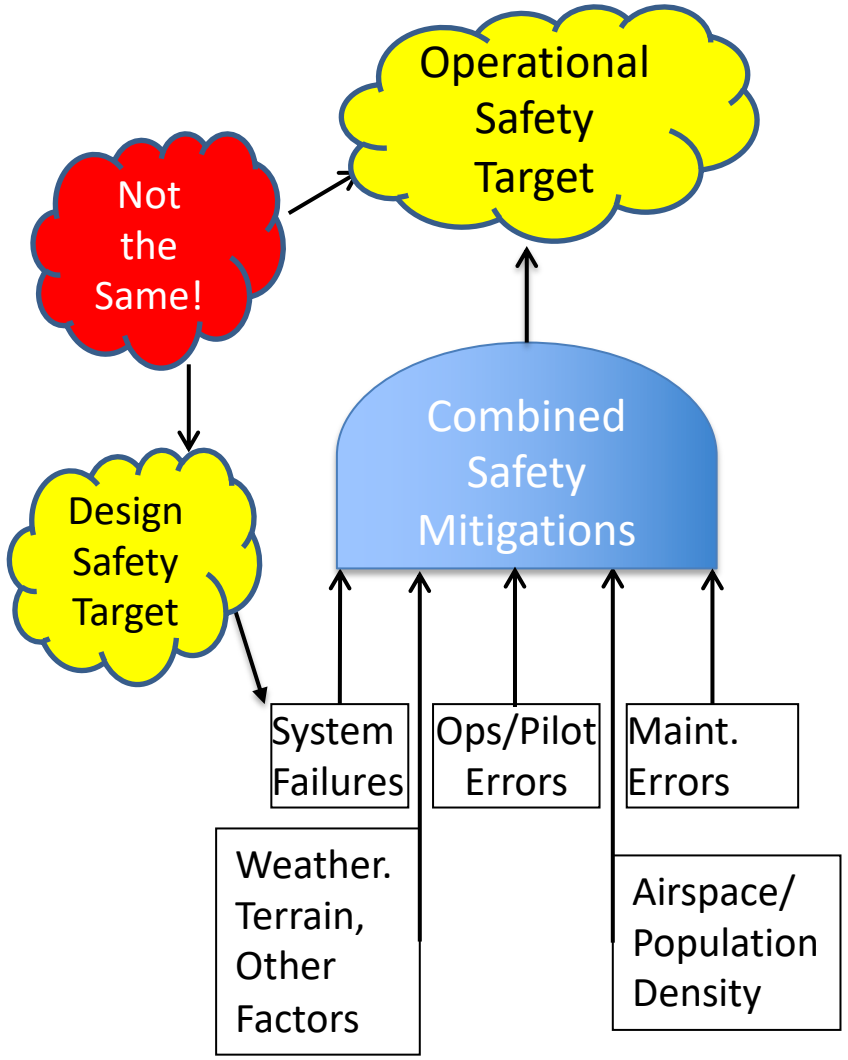
Kevin Rodgers, Northrop Grumman

Moderator – Wes Ryan, NASA

Panel Discussion: Setting the Stage For Defining Safety

- What is Safety? = Loss of Life? Loss of the Aircraft?
- Design Safety and Operational Safety - Are they the Same?

- Systems, airspace, ops, maintenance, & pilot error all feed into operational safety
- How do safety targets get applied to aircraft automation vs. operational automation?
- Some try to fix top level ops safety target with increasing $10E^{-X}$ for system failures and design
- We can design to a probability, but not all risk mitigation comes from design



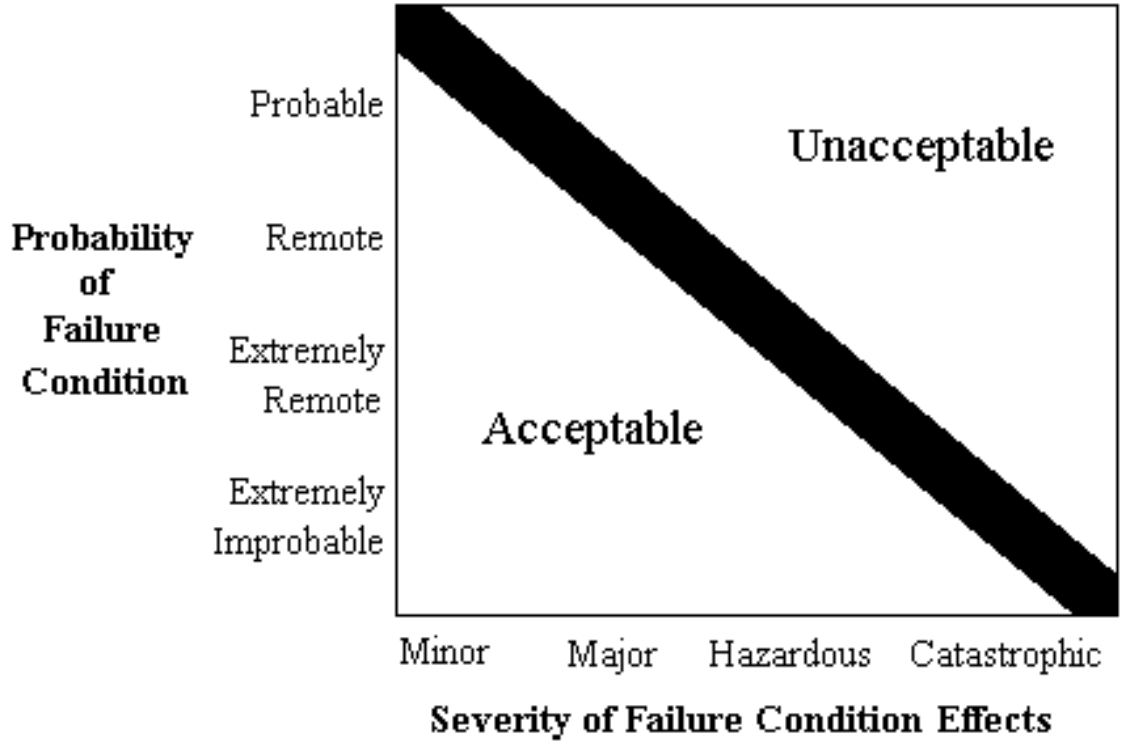
Setting the Stage: Defining Safety Expectations

- The move from aircraft function pass/fail to probabilistic analysis has had a profound positive impact on safety but is also a double edge sword.
- Often the desire to model a probability leads to multiple-layers of conservative estimates that lead to a “safety stacking” problem.

EFFECT=CATASTROPHIC
UNACCEPTABLE

EFFECT≠CATASTROPHIC
ACCEPTABLE

VS
(1973)



Basic Functional Performance Pass/Fail

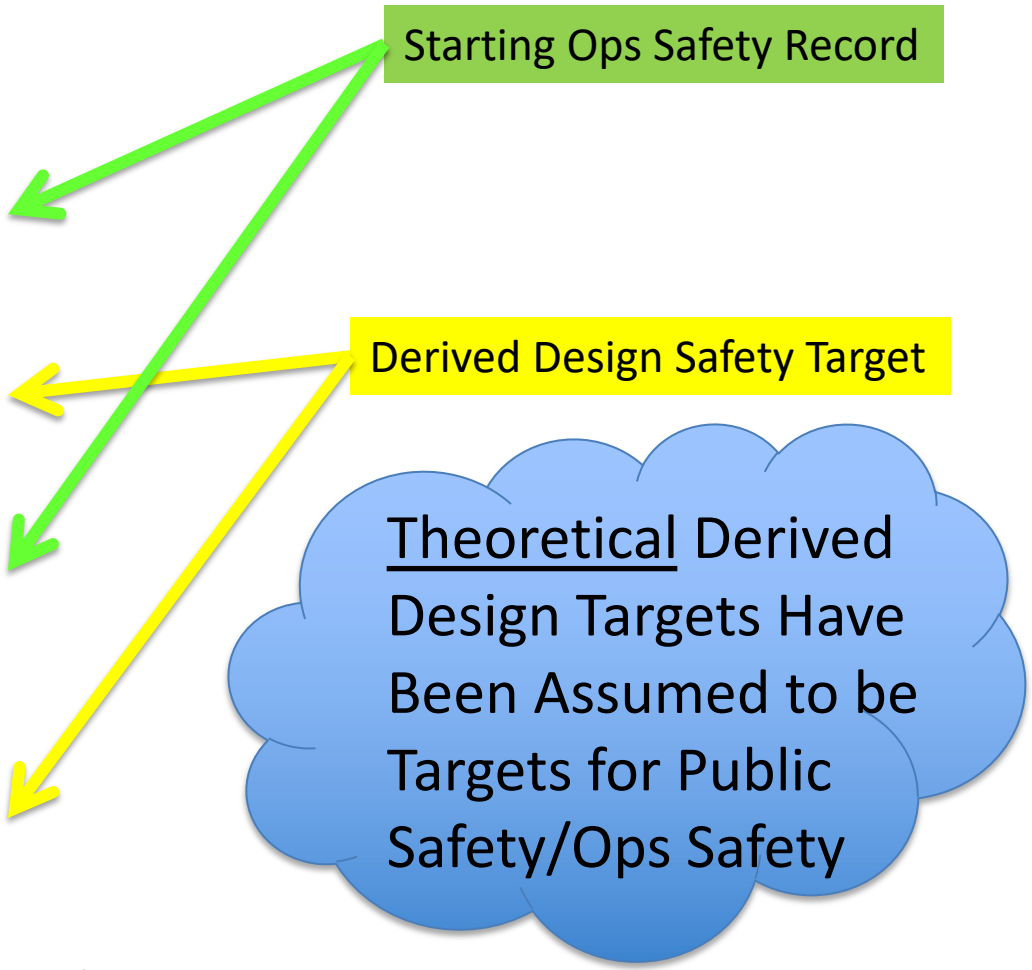
Inverse Relation – Likelihood and Severity

Background: So Where Did 10^{-9} Come From?

Ref: AC 23-1309-1C Published 1999
and AC 23.1309-1D published 2009

- *TRANSPORT* CATEGORY AIRPLANES
  - Fatal accident rate at time of rule 10^{-6}
  - Data showed ~10% caused by system failures 10^{-1}
  - Assume 100 catastrophic failure conditions 10^{-2}
  - Results in probability 10^{-9}

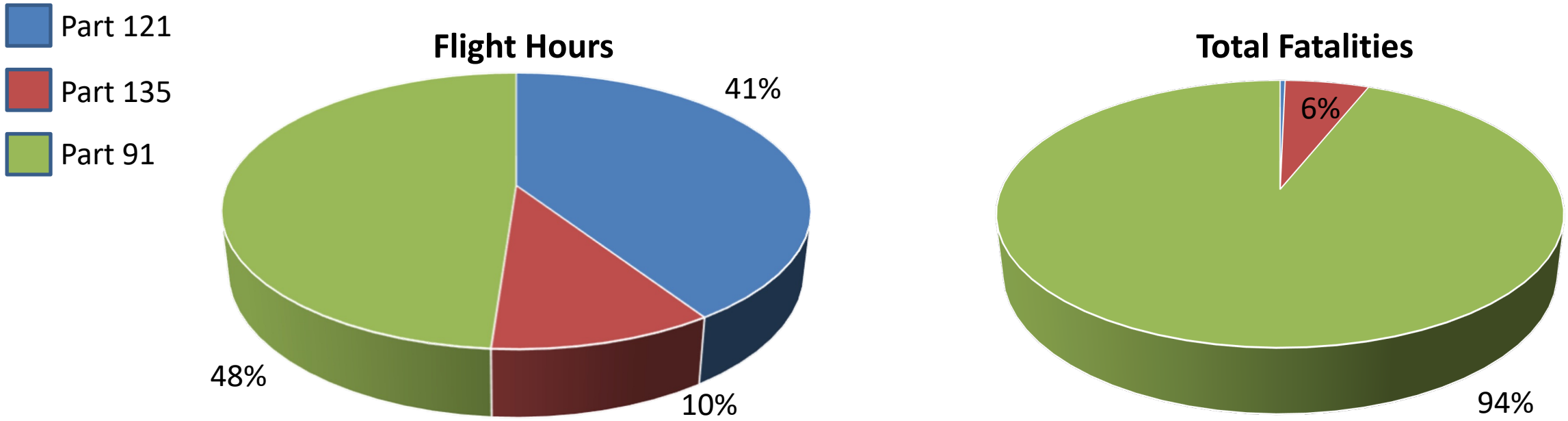
- *SMALL SINGLE-ENGINE* AIRPLANES
  - Fatal accident rate at time of rule (IN IMC) 10^{-4}
  - ~10% caused by system failures 10^{-1}
  - Assume 10 catastrophic failure conditions 10^{-1}
  - Results in probability 10^{-6}



- Goal: Fatal accident rate should NOT INCREASE from new equipment or automation

Background: Overall Aviation Safety 2010-2020

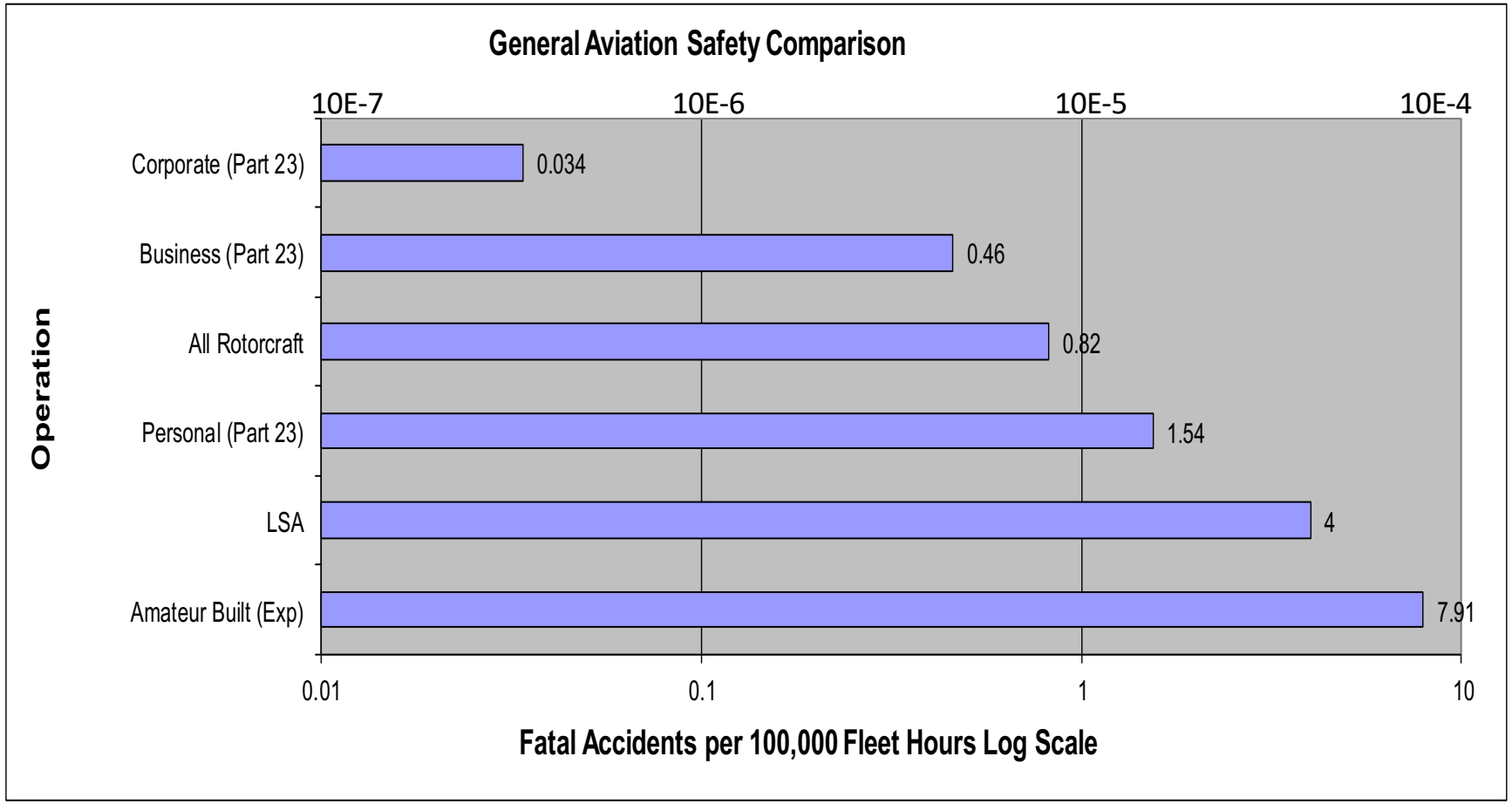
- Part 121 - Scheduled air carrier operations - 191,735,000 Flight hours (2010-2020) 83 Billion Flight Miles (16 Total Fatalities)
- Part 135 - Commuter operations and on-demand operations (charters) with 30 or fewer seats or a maximum payload capacity of 7,500 pounds – 48,821,000 Flight hours (267 Total Fatalities)
- Part 91 – General aviation – 229,898,000 Flight Hours (4,386 Total Fatalities)



Data - Courtesy Loyd Hook, University of Tulsa, Used with Permission

Target – Improve Ops Safety With Technology

- We want AAM/UAM to improve safety over GA through automation and electric propulsion, but too high of a target safety level could be a barrier to success
- Avoid raising bar on premise of “It’s new”, or “complex” - GPS used to be “new”



Operational Safety Target

≠

System Level Safety Target for Design & Certification

Panel Discussion: Setting the Stage For Measuring Risk/Safety

There are many methods for analyzing & measuring risk and defining expected safety targets

- ARP 4754 and 4761
- JARUS SORA
- STMP
- FAA D&R Process – Service History
- Others

Need: What Should the Global Method/Standard be and Why?

Why has there been such a large difference of opinion on the "Right" method? Design vs. Operational Focus? SUAS vs. Larger UAS?

Panel Discussion: Background: What About Fleet Risk?

Safety Targets Often Vary When Fleet Size Varies

Common Comment/Question:

- If I have 100 times more airplanes in my fleet, do I need to meet 100 times the design or operational safety target?

Why is this a source of confusion?

We have many publicly accepted transportation related risks that to not meet aviation safety levels. Why would every new aviation operation be held to commercial transport safety levels – public risk?

Has Ground Risk evaluation in risk analysis made things worse?

Poll #2 – Measuring Safety – Fleet Risk

Should Probabilistic Targets Be Per Flight/Individual Aircraft or Should a Larger Fleet Meet a Higher Standard?

- Individual - Per Flight
- Individual – Per Flight Hour
- Fleet Calculation – More Aircraft = Higher Safety Target
- Other?

Panel Discussion: Making a Safety Case to Civil Authorities

Design and Ops Safety Expectations Vary with CONOP, Aircraft Performance/Size, and Intended Airspace

- Describe your experience making a safety case to Authorities (Civil or Military) for Design and Operational Safety

Experience has shown that industry pressure combined with FAA/industry partnerships so they gain familiarity with ops safety for a new idea can lead to success.

- The FAA cannot certify ideas or concepts
- They need tangible products to evaluate
- How can NASA R&D and govt./industry partnerships help move things ahead?

OPEN Q&A FROM AUDIENCE WITH THE PANEL

SUPPORTING SLIDES

Design Certification Safety Targets – ARP 4761

TABLE 1 - Failure Condition Severity as Related to Probability Objectives and Assurance Levels

Probability (Quantitative)		Per flight hour 1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic
	JAA	Minor		Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants		- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants	- all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D		Level C	Level B	Level A

Note: A "No Safety Effect" Development Assurance Level E exists which may span any probability range.

Evolution of Ops Enabled by Technology

Origins of Visual Flight Rules (VFR)

See and Avoid

Visual Separation

Flexibility ✓
Access ✗

Radio Navigation

"Airways"

Origins of Instrument Flight Rules (IFR)

Increased Collision Risk

Flexibility ✗
Access ✓

"Airway" Traffic Control (ATC)

Procedural Separation

Voice Communications

Radar Surveillance

Radar Separation

Global Precision Navigation

Advanced Avionics

Traffic Management Automation

Data Communications

Initial Trajectory-Based Operations

CAUTION!
The Future of Aviation Mobility is:

Capacity ✓
Flexibility ✓
Access ✓

Capacity ↑
Flexibility ✗
Access ✓

STRIVES 20220013666

Example – Technology Maturation

NASA Paper: [Visual advantage of enhanced flight vision system during NextGen flight test evaluation]

Advisory
Supplemental, or Emergency Only

Pilot is Primary For Safety

Assistive Technology
System Provides Certified/Accurate Data

Shared Responsibility - Pilot is Still Primary For Safety

Mature Technology
System Has Proven Reliable Use in Service - Provides Certified, Accurate Data

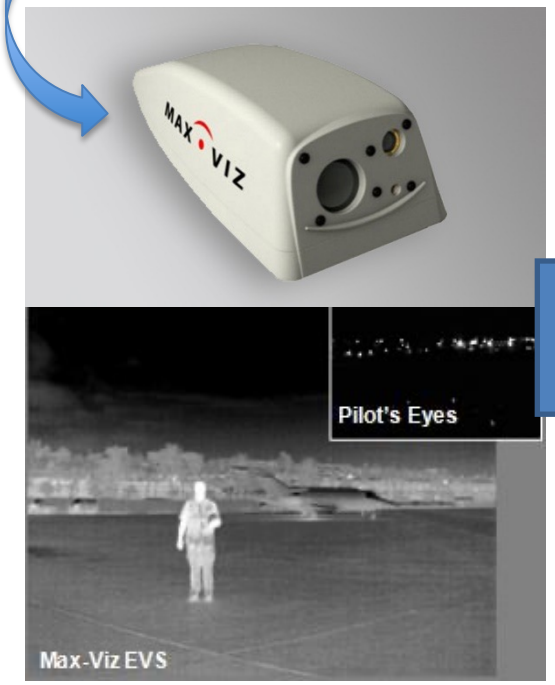
Pilot is Still Primary For Safety

Technology For Operational Credit
System Has Proven Reliable Use in Service - Provides Certified/Accurate Data – Regulations Changed Based on Proven Maturity to Allow Credit for Use

Pilot is Backup to Proven Technology

"Responsible" Technology
System Has Proven Reliable Use in Service - Provides Certified/Accurate Data Without Reversion to Pilot Backup for Sufficeint Number of Hours - Regulations Changed to Recognize Technology as Primary for Intended Use

Technology is Primary For Safety



Tech Maturation

Regulatory Change

Lower Approach Minimums

Technology Not Approved for Autoland

Safety Case Requires Entire Capability to Be Considered

New concept, ability, expertise, or proficiency

Task, role, and/or system effects which enable a *Capability*

Equipment including HW/SW which enables *Function/ Service*

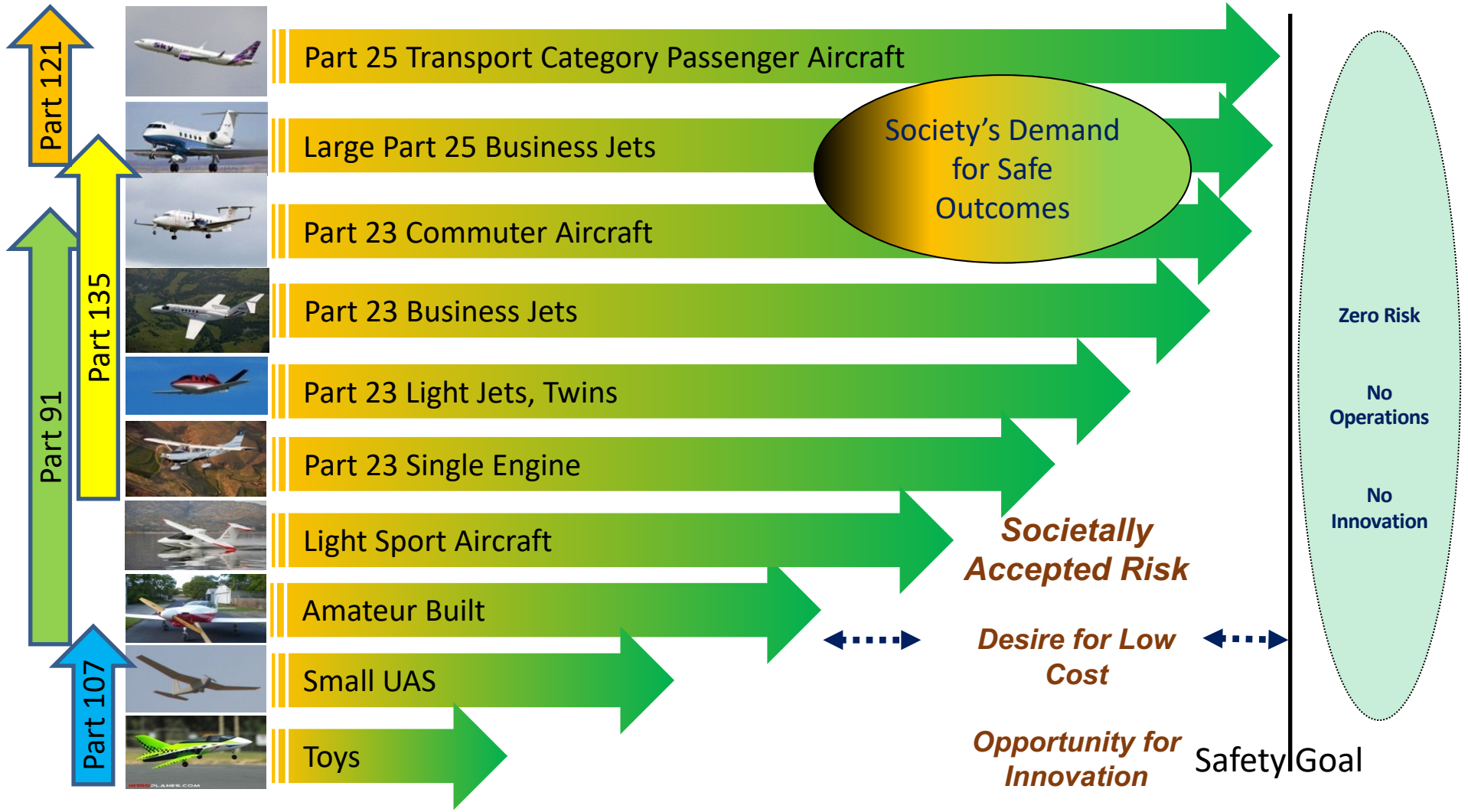
Information sources used by *Technology*

Must assess maturity, integrity, reliability, availability, etc. of data sources & technology to implement an intended function in support of a new capability

STRIVES 20220013561

Notional Design Certification Safety Targets

Risk Based Approach to Innovation & Certification

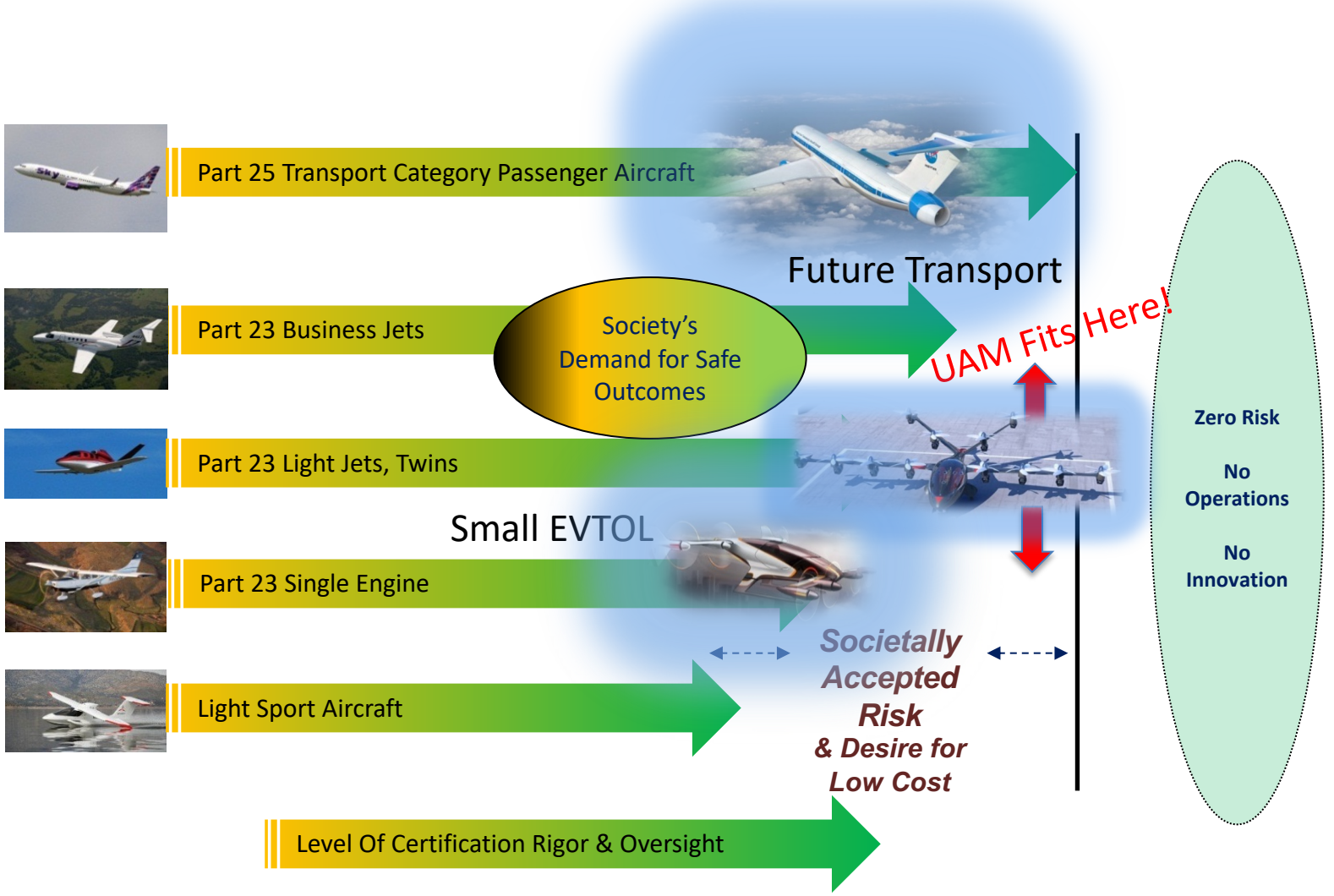


Rigor of Certification Oversight Follows Risk-Based Structure

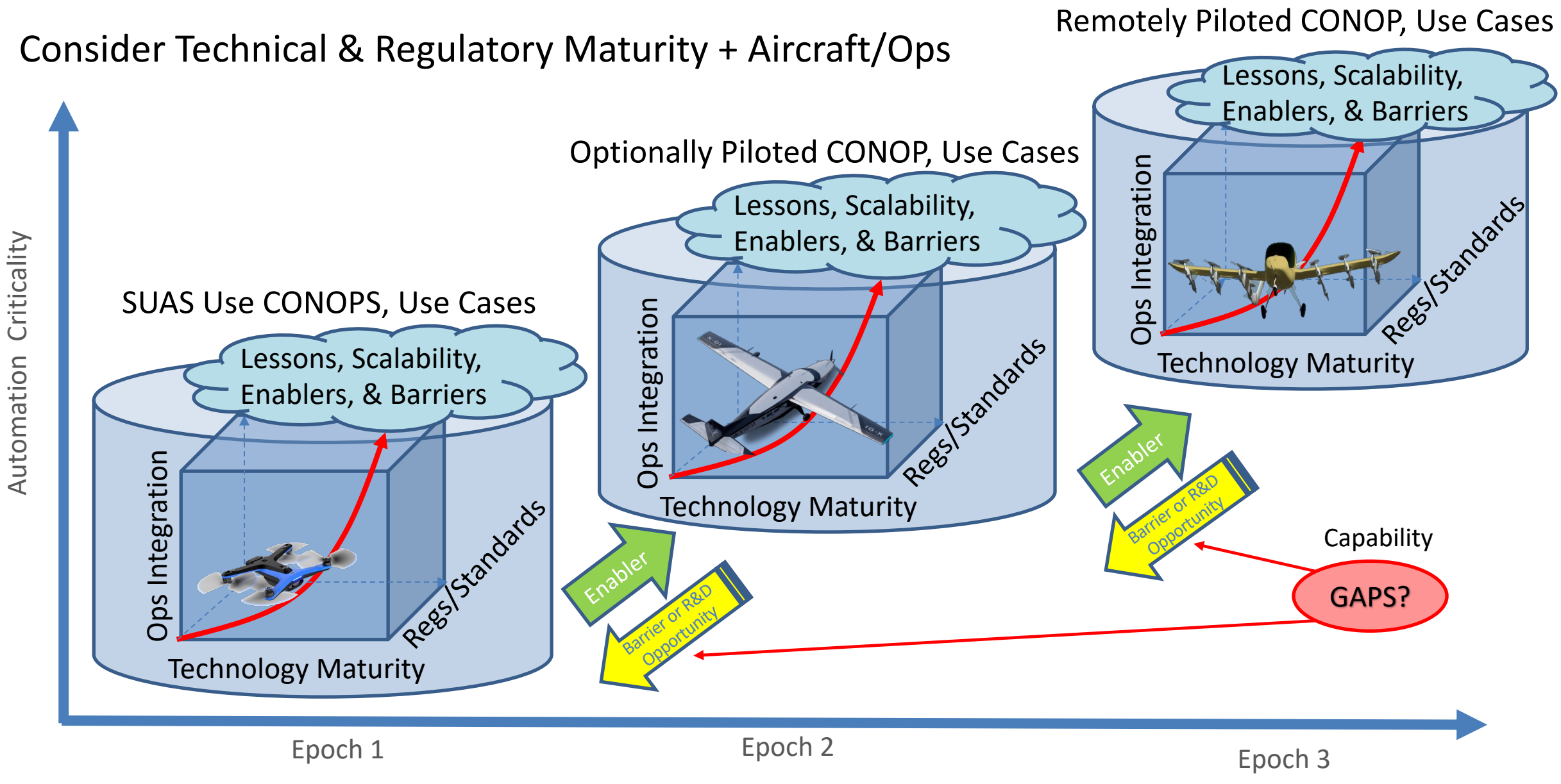
Aircraft, and Intended Use Must Be Considered

Setting System Safety and Design Expectations

- Too High of Notional Safety Expectation Will Stifle UAM Before it Gets Started
- FAA Risk-Based Certification Requires Right Level of Certification Rigor and Oversight
- We Already Have Tiered Requirements in Existing Cert and Ops Rules



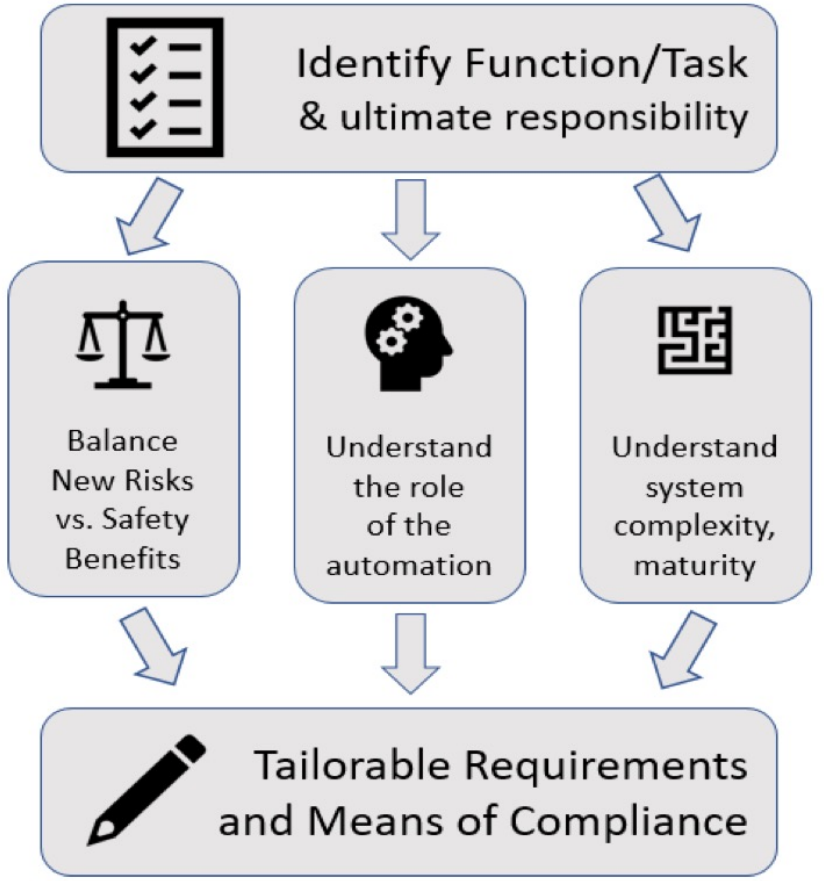
Different Expectations and Evolution Paths



STRIVES 20210022451

Automation Maturation – Industry Example

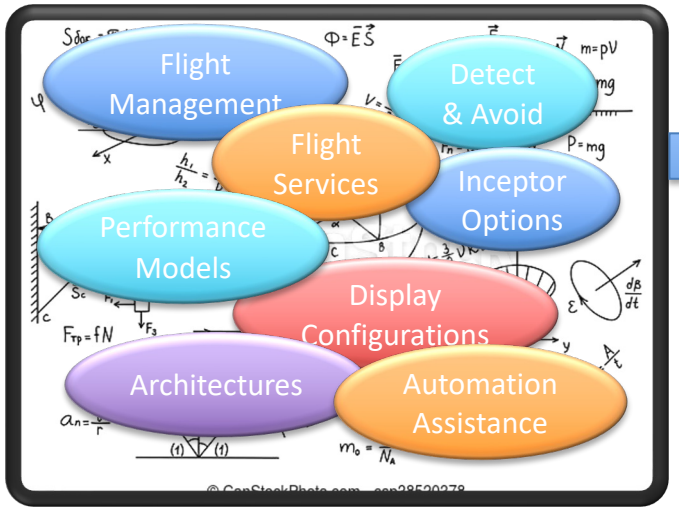
- Introduce Automation In Low-Risk Use Cases First, Where Appropriate
- Collect Data & Use Data to Develop/Validate Models
- Analyze Models for Higher Risk Safety Cases to Evolve
- “Build a Little, Test a Little” - Iterative Loop
- Models for Physical Problems Easier to Develop/Mature Than Models for Decision Making and Perception Functions
- Move Technical Maturity Forward for Specific Functions – Combine Functions to Reach Specific Operational Goals for Autonomy



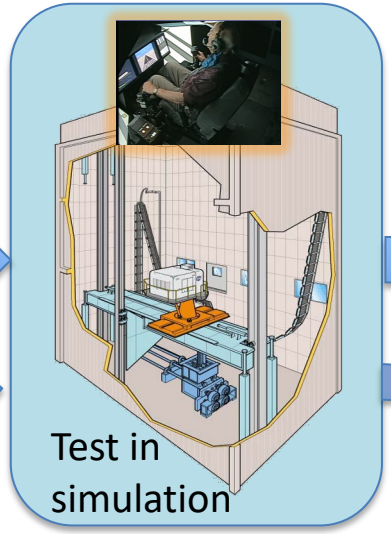
From ASTM AC 377 TR

Automation Maturation Process – NASA Example

Technical Challenge:
Develop and evaluate an initial, integrated suite of key automation functions to enable simplified piloting in urban environments and propose recommendations to enable certification and approvals for the selected concepts.



Use industry-representative models & technologies



Validate in flight
National Campaign (NC)/Integrated Automated Systems (IAS)

Capture Requirements

Identify common techniques for evaluation of performance, handling and safety

Deliver findings to inform development of System Concepts, Standards, Certification requirements and Means of Compliance

Deconstruction of Functional/Technology Capability

Functionally Based Approach to Product Development

- Intended Function & Use Case
- Identify Available Technology, Procedures
- Set Clear Roles for Human and Machine
- Identify Development & Operational Path For Use
- Flight Test & Data Collection
- Pass/Fail, Showing of Compliance

Functionally Based Approach to Policy & Regulation

- Applicable Regulations, Policy, Procedures
- Do They Need To Change?
- FAA Rulemaking
- Industry Standards

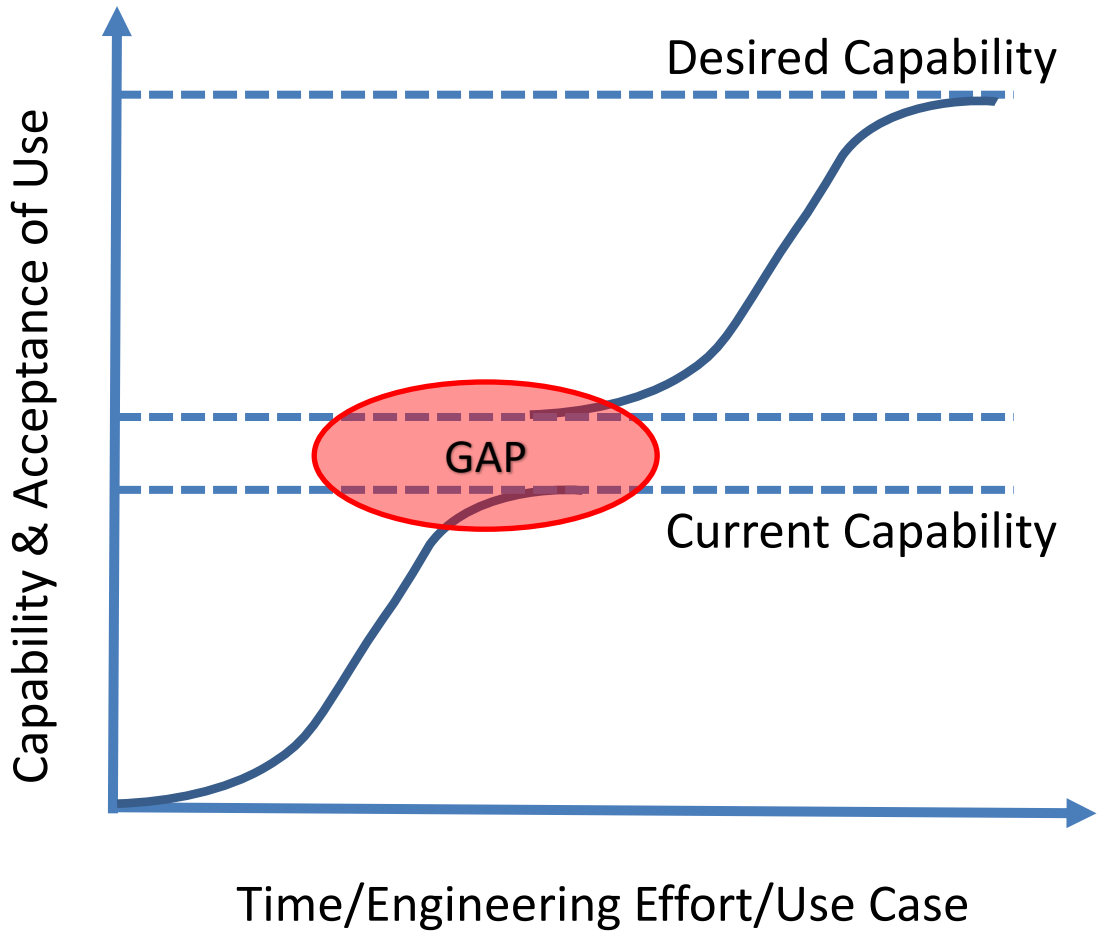
Consider Technology and Policy. Are Development Timelines and Assumptions Viable?

Proposed Gated Process for Evaluating Capability/Function/Technology/Data

Gate	Action/Evaluation
0	Identify an intended function for automation including the context – Intended use (e.g. operational context and/or phase of flight, and functional interfaces/dependencies)
1	Explain the potential benefits or incentives of automating the proposed function (e.g. safety enhancement, operational enhancement, and economics). Identify any potential risks, limitations, or barriers to automating the proposed function
2	Define how the intended function is currently completed/accomplished in operations and describe how it would be completed/accomplished once automated. Include human responsibilities and authority and how they could change and other system interfaces or dependencies when comparing.
3	Define the required information, processing, and outputs necessary to automate the function.
4	Identify candidate example technology products that may be capable of automating the function
5	Identify gaps in the current technology products to perform the function, and what operations the current technology could enable now
6	Identify the required maturity level of a technology product for it to achieve the intended function. Describe any differences in the level of maturity that may be appropriate depending upon aircraft size (i.e., normal category, transport category), kind of operation (i.e., cargo, passenger-carrying), or any other appropriate risk consideration.
7	Identify a path from current technology capabilities to the future technology capabilities necessary to achieve the identified maturity level(s).
8	Identify the applicable regulations/policy/standards/guidance (i.e., aircraft certification, operational, airman, ICAO) related to the current function.
9	With reference to Gates 2 and 8, identify what regulations/policy/standards/guidance may need revision and where new regulations/policy/standards/guidance may need to be developed to certify an aircraft with the technology and authorize/enable its use in operations.

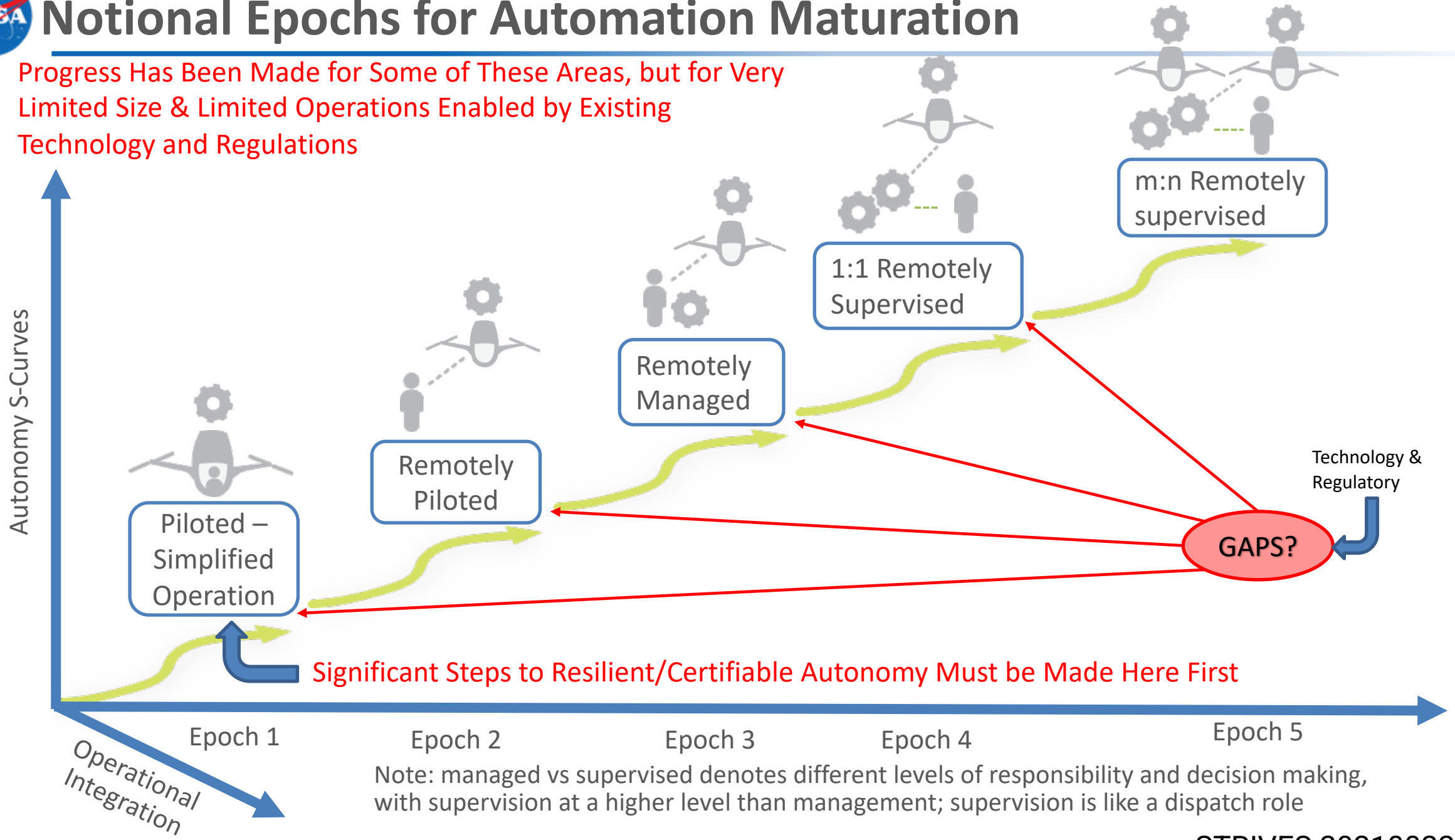
S-Curve Epochs – Maturity & Discontinuity

- Gaps in Capability May Limit Growth Towards Ultimate Goal/Use Case
- Gaps Can Exist in Technology, Regulation, and/or Operational Capability
- Consider the Level of Expected Integration vs. Demonstrated Capability
- Technology Gaps Must be Overcome by Data Collection and Demonstration in Real-World Scenarios – Catch 22
- Regulatory Gaps Present Similar Challenge - Overcome by Data



Notional Epochs for Automation Maturation

Progress Has Been Made for Some of These Areas, but for Very Limited Size & Limited Operations Enabled by Existing Technology and Regulations

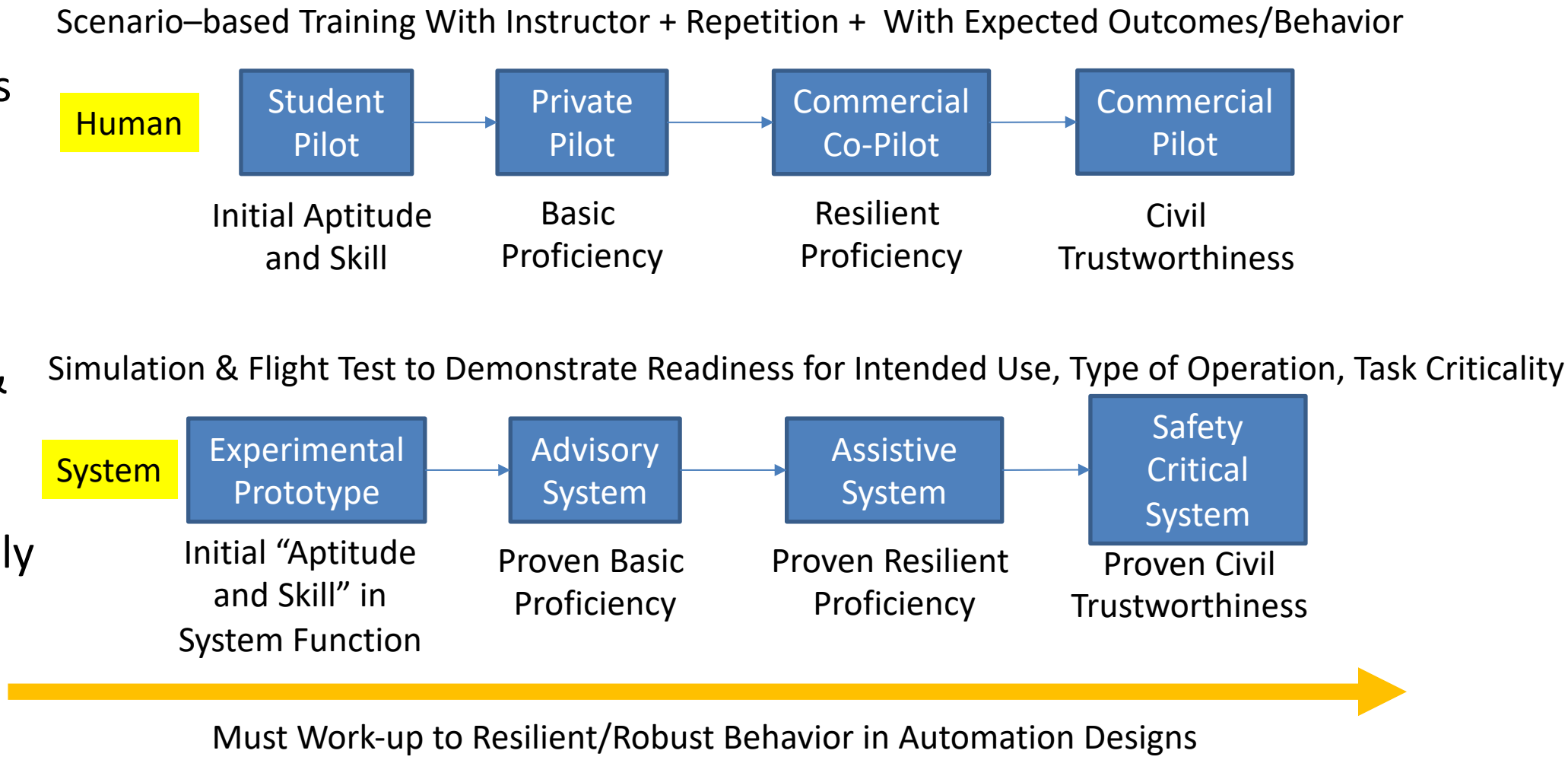


Note: managed vs supervised denotes different levels of responsibility and decision making, with supervision at a higher level than management; supervision is like a dispatch role

STRIVES 20210022451

Focus on Behavior/Rule Based Outcomes

- Pass/Fail Criteria for Specific Tasks
- Focus on Intended Function
- Build In, Test Proficiency & Robust Function
- Criticality Only Increases as S-curve Reaches Maturity



STRIVES 20210013394

Progression of Design Towards Maturity & Certification

- Methodical Progression from Prototype, to Initial Function with Human Monitoring/Backup, to Safety Responsible Function
- Common Framework for Analyzing Each Step Towards Proven Capability