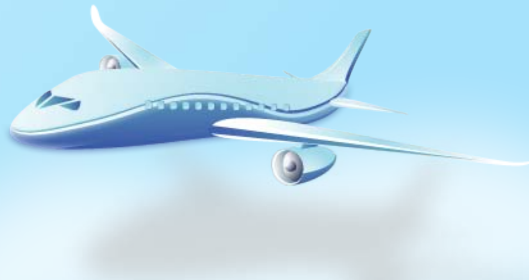
Cognitive Engineering Center

Georgia Institute of Technology

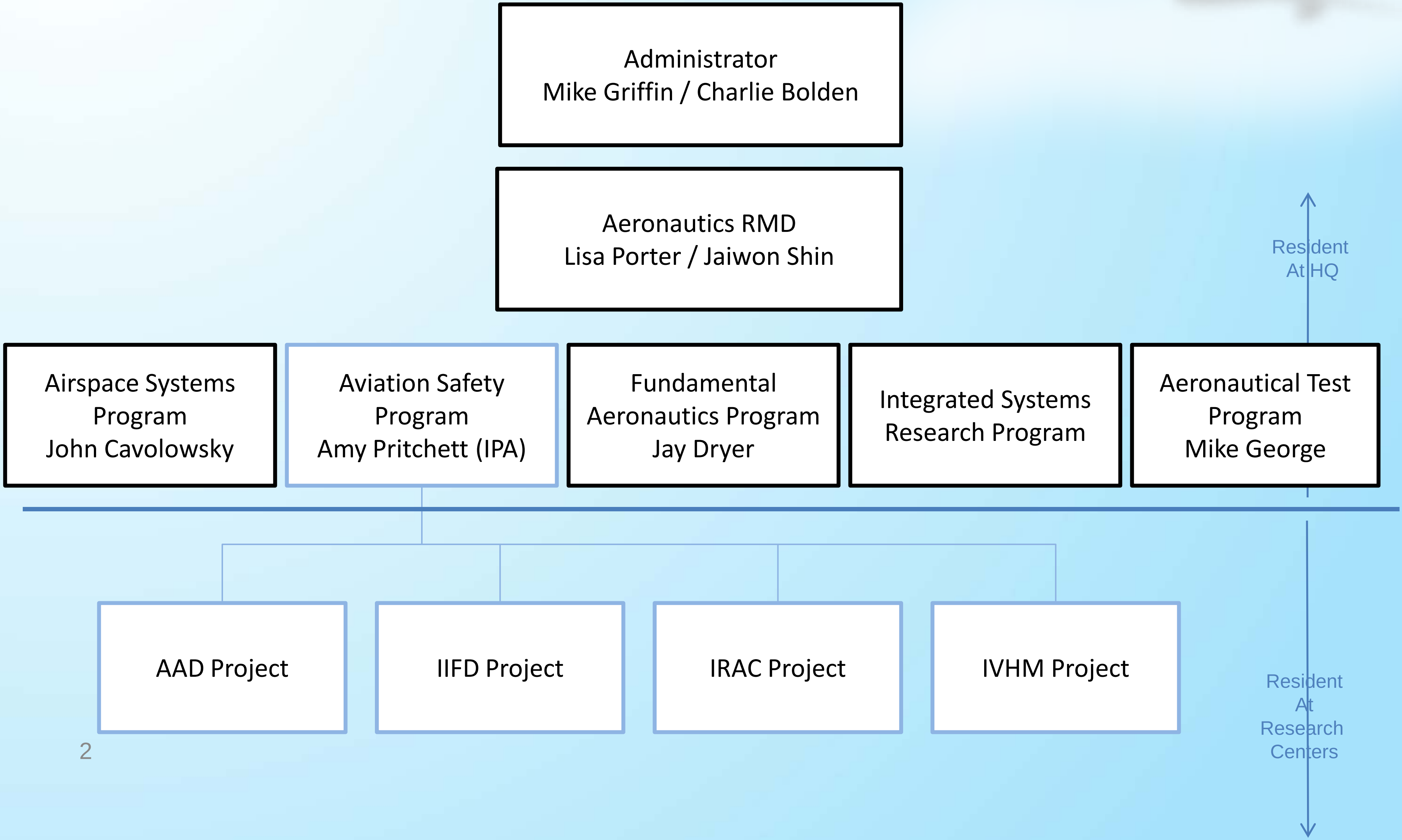
The Intersection of Technology and Policy in Aviation Safety

Amy R. Pritchett

November 1, 2011



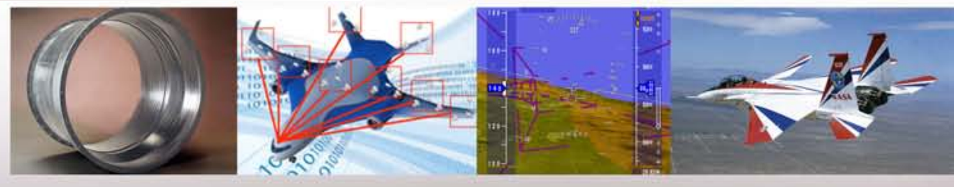
Background: The Position



National Aeronautics and Space Administration

Future Directions in Aviation Safety: Musings of an IPA as She Cleans Out Her Office

Dr. Amy R. Pritchett
Director, NASA Aviation Safety Program



Annual Technical Conference
November 17-19, 2009

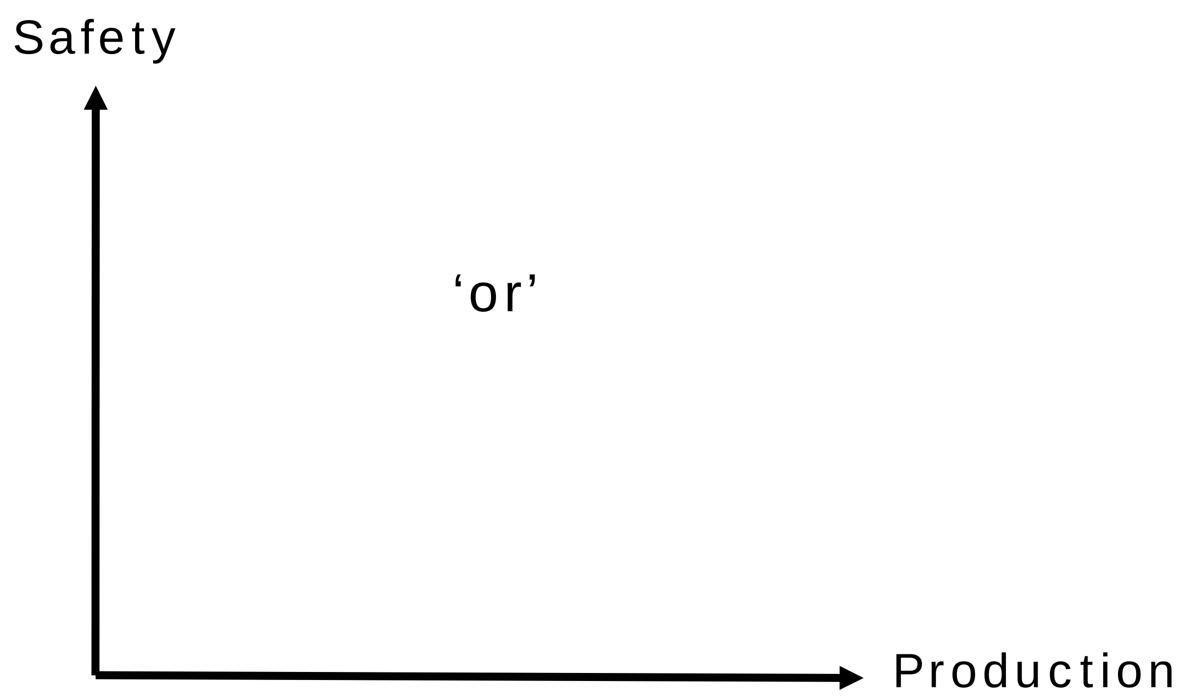
Why a Separate Safety Program?

Some what pessimistically, James Reason and others have discussed the inherent trade-off of ‘safety versus production’

Safety ‘versus’ Production

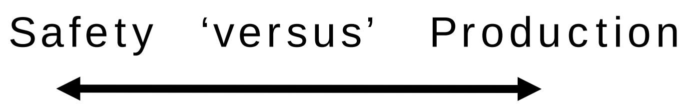
Why a Separate Safety Program?

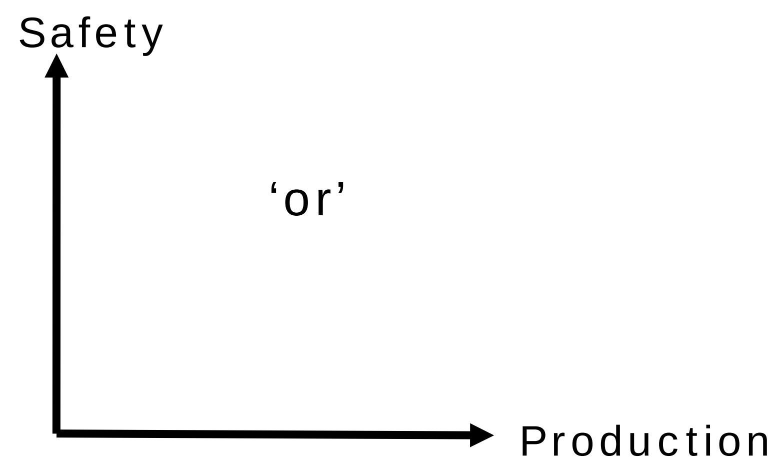
Some what pessimistically, James Reason and others have discussed the inherent trade-off of ‘safety versus production’



Why a Separate Safety Program?

Some what pessimistically, James Reason and others have discussed the inherent trade-off of ‘safety versus production’





Either way, the role of a safety program is not just to address safety, but to provide the knowledge to effectively manage this trade-space

Without Knowledge of This Trade-space…

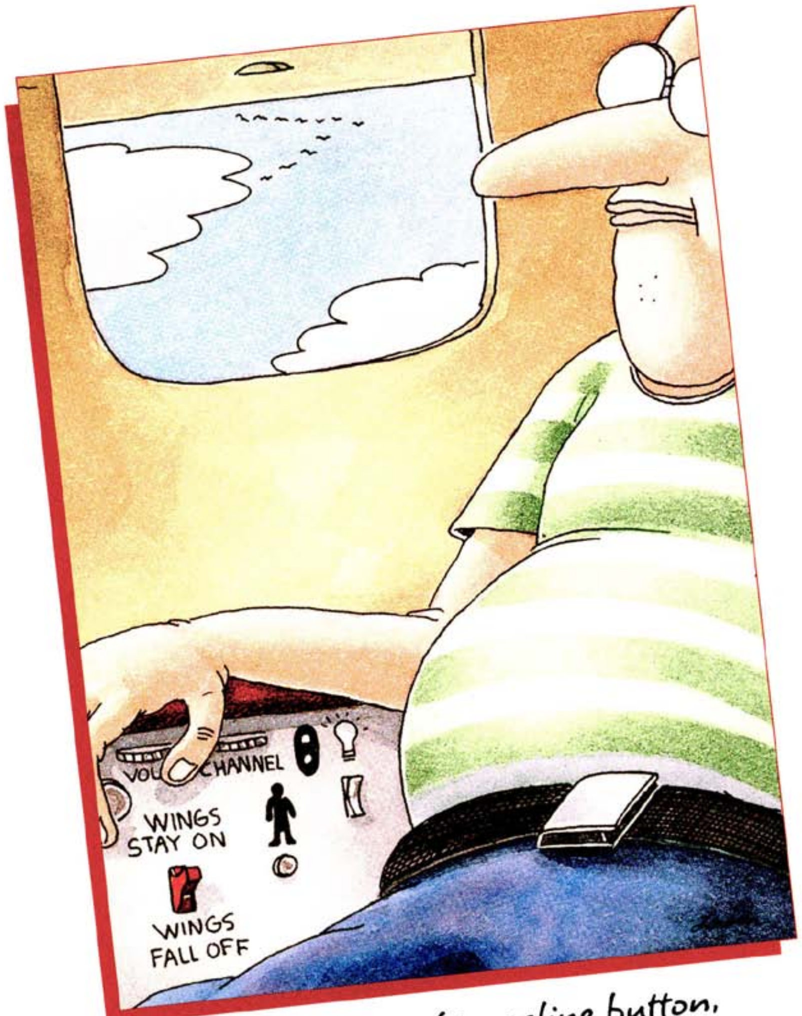
… somebody will need to make a decision whether to implement a new function or capability. (In aviation this is ‘certification risk’)

A Simple View… Single-Point Failures

- The simplest viewpoint considers accidents the response to single, identifiable faults and failures
- A good starting point is to eliminate the potential for single-point failures, or simple error chains…

But this alone won't get us the safety levels we need!

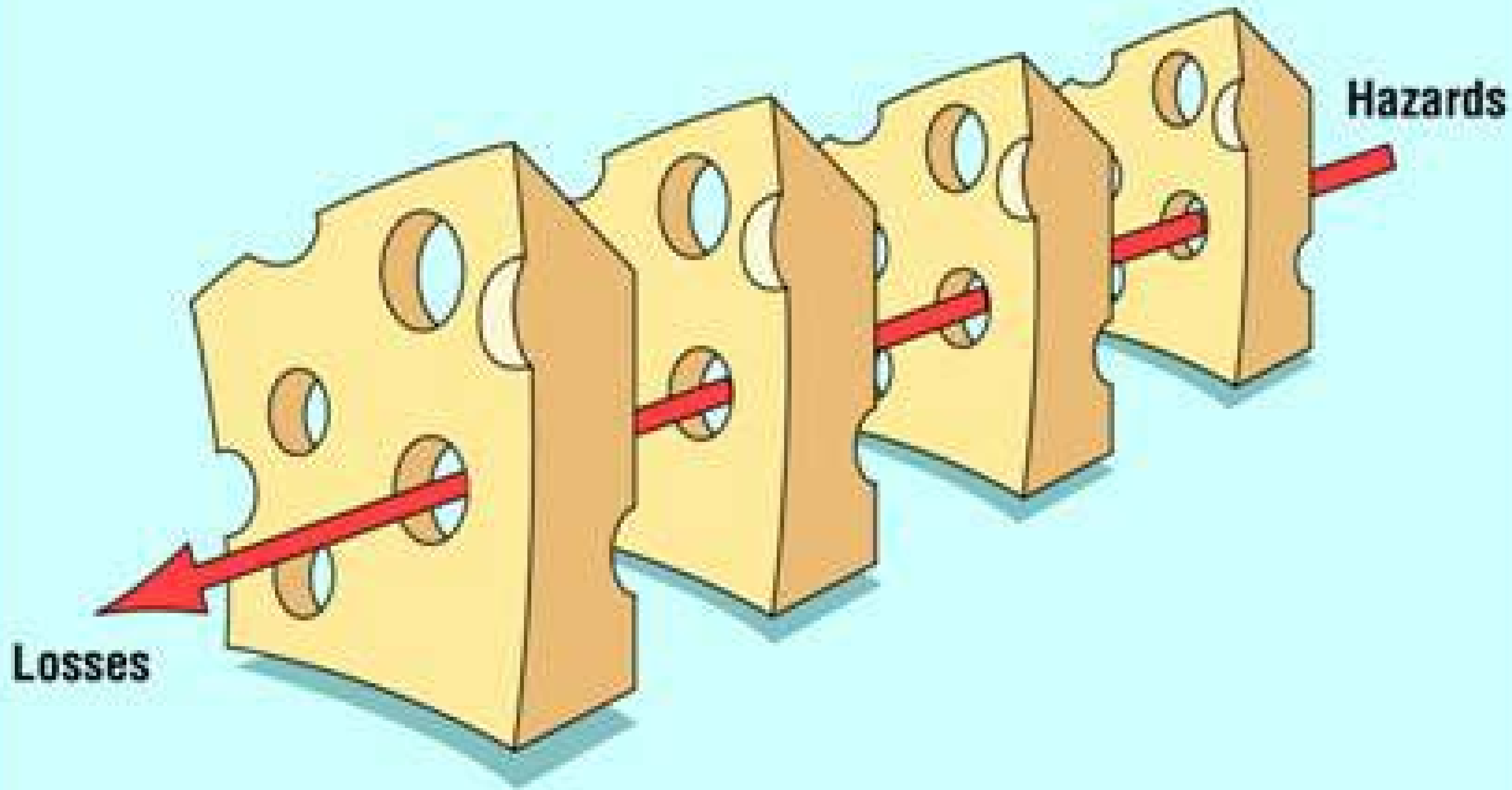
$$p_{accident} = p_{failure1} + p_{failure2}$$



Fumbling for his recline button, Ted unwittingly instigates a disaster.

Building Up – Reason's 'Swiss Cheese'

Organizational and technical factors create holes in safety nets



$$p_{accident} = p_{failure1} * p_{failure2} * p_{latent1} * p_{latent2}$$

Building Further – Strong Coupling

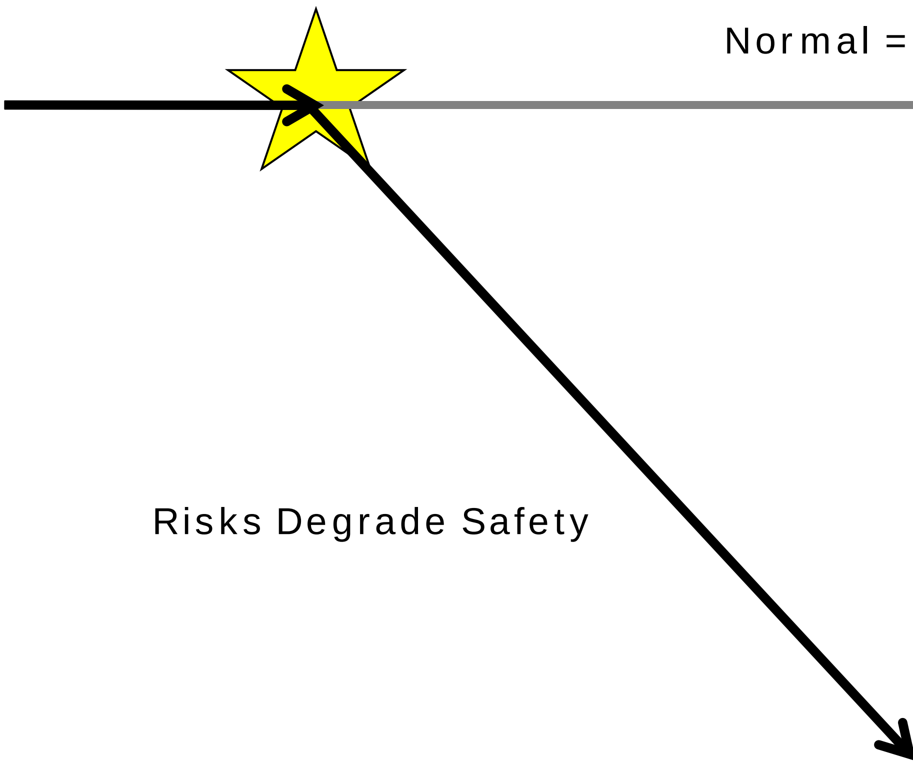
- What if one weakness aggravates the potential for another?

$p_{accident} = p_{failure1} * p_{failure2}\{failure1\} * p_{failure3}\{failure1 \,\&\, failure2\} * \ldots$

- Mechanisms then exist for cascading and compounding failures developing non-linearly into accidents
  - These behaviors can't be captured with fault trees!

Which Does Classic 'Risk' Modeling Lead?

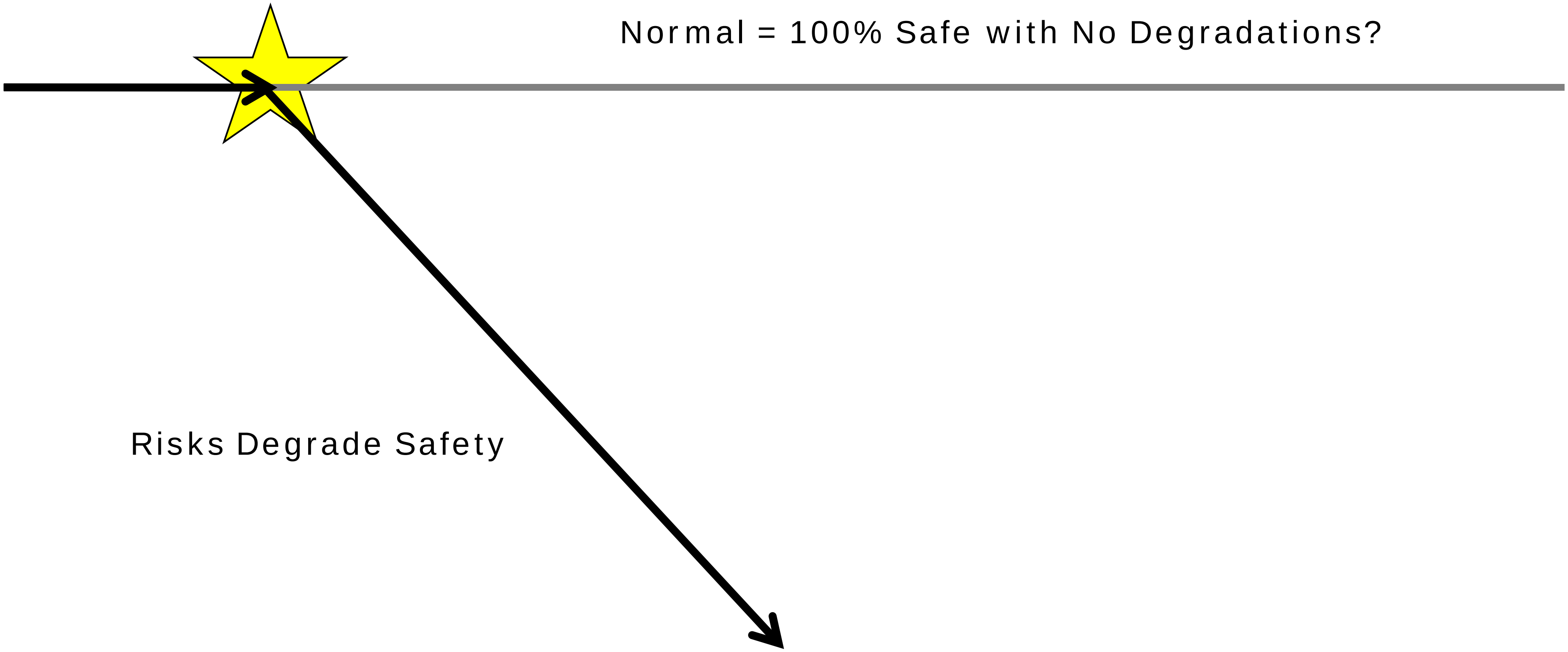
Normal = 100% Safe with No Degradations?



Corollary: Eliminate Risks, Disturbances & Degradations – Stick to Your Normative State – and Safety is Ensured

Risk Models Can Only Model the Negative – They Can't Model What Restores Us to Safe Operations

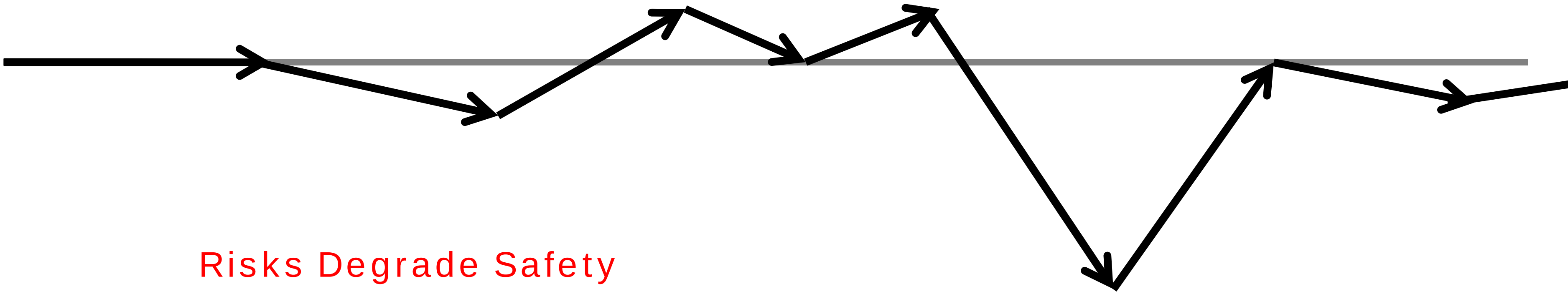
Modeling Resilience



Modeling Resilience

Normal = Constant Variation

Other Processes Restore Safety!

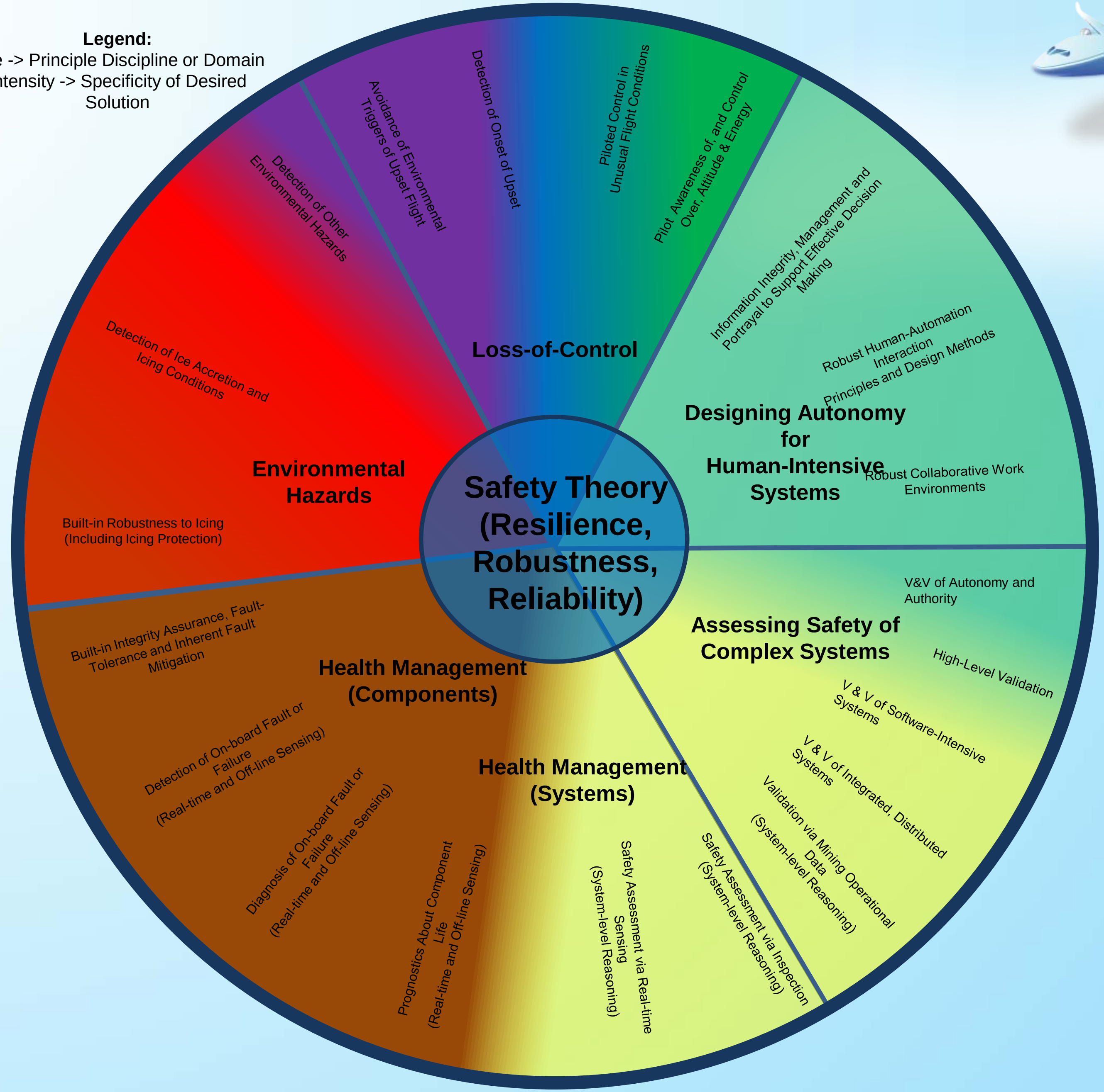


Risks Degrade Safety

Success or Failure?

Which Aspects of this Accident Should We Focus On?

Legend:
Hue -> Principle Discipline or Domain
Intensity -> Specificity of Desired Solution



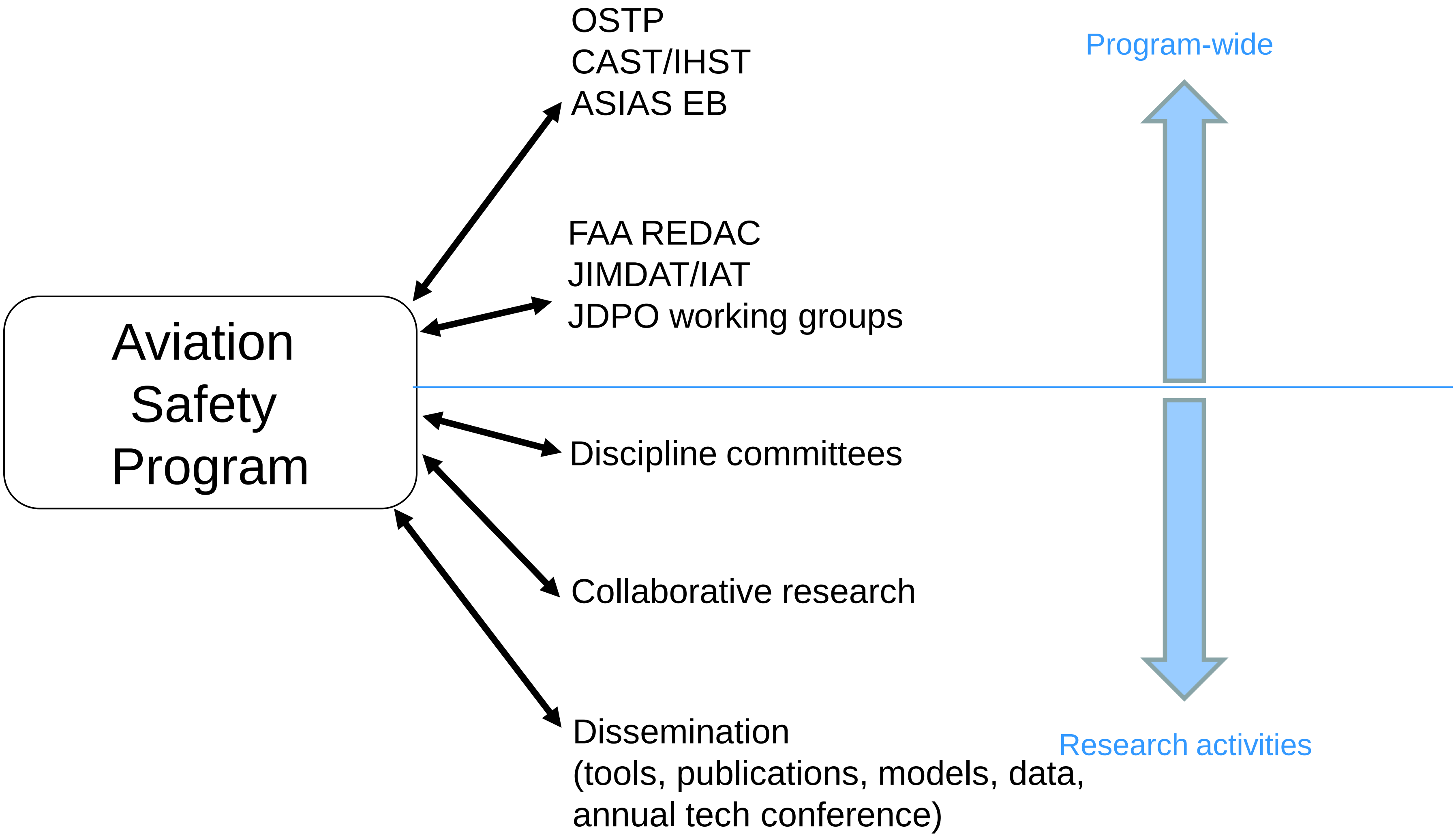
Process for Identifying Emerging Research Needs

Major function of program office is to frequently review existing and proposed research for:

- Consistency with and support of clear national need
  - Current safety technical and operational problems
  - Potential future safety technical and operational problems
  - Safety constraining innovation
- Need for long-term fundamental science and engineering research
- Alignment with unique NASA charter
- Other selection considerations
  - Appropriate resources, workforce and facilities
  - Sustaining commitments

Must ensure flexibility to consider new research areas and urgent problems

Interacting With our Community



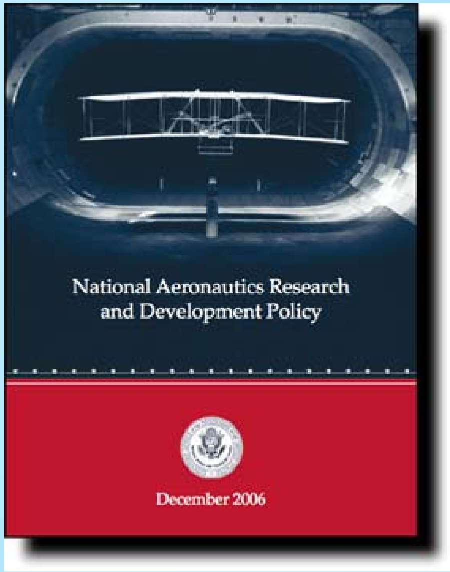
National Aeronautics R & D Policy & Plan

What research is vital to civil aeronautics?

And what should the government do?

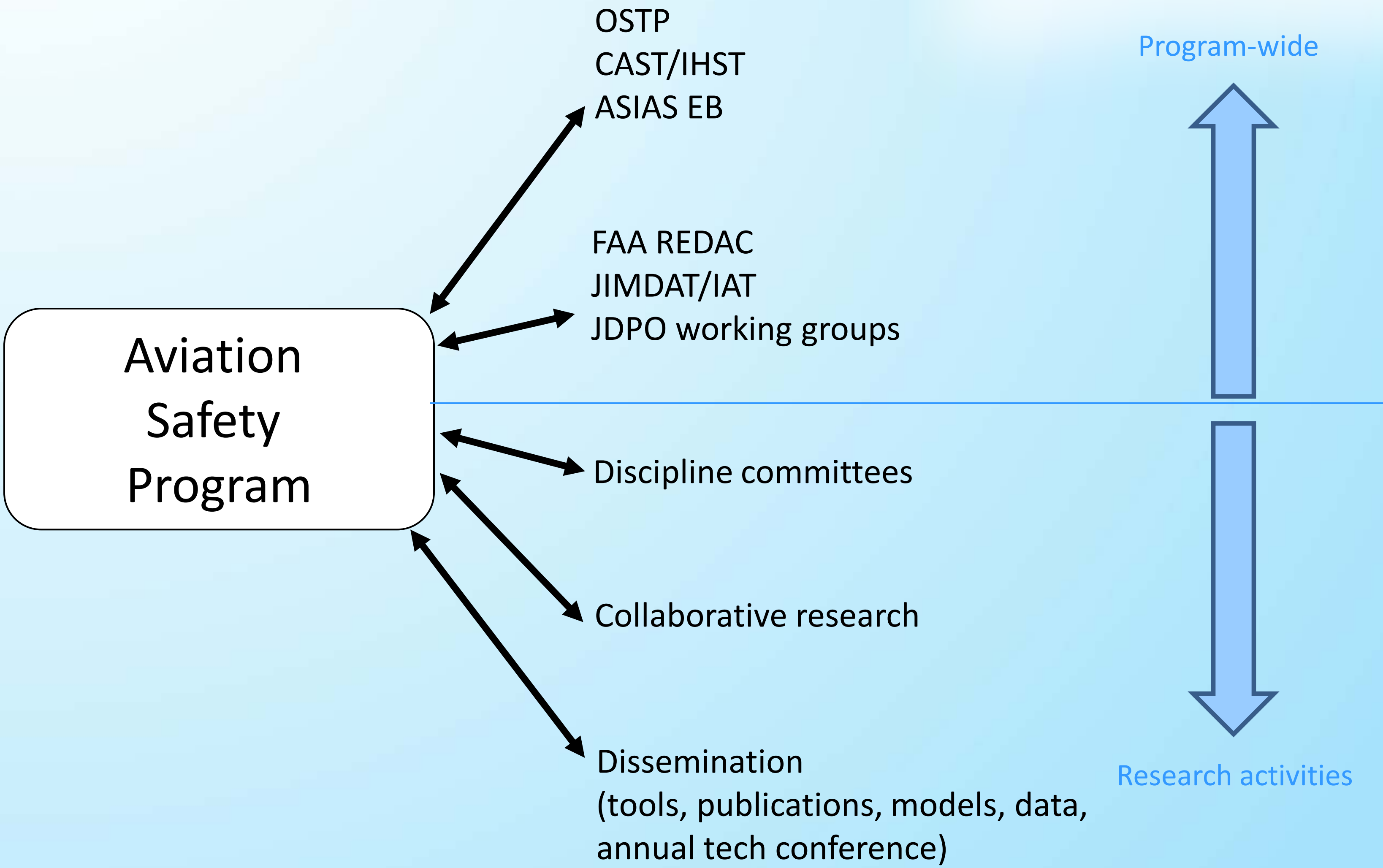
What "infrastructure" should be maintained as a national resource?

And how is it costed…



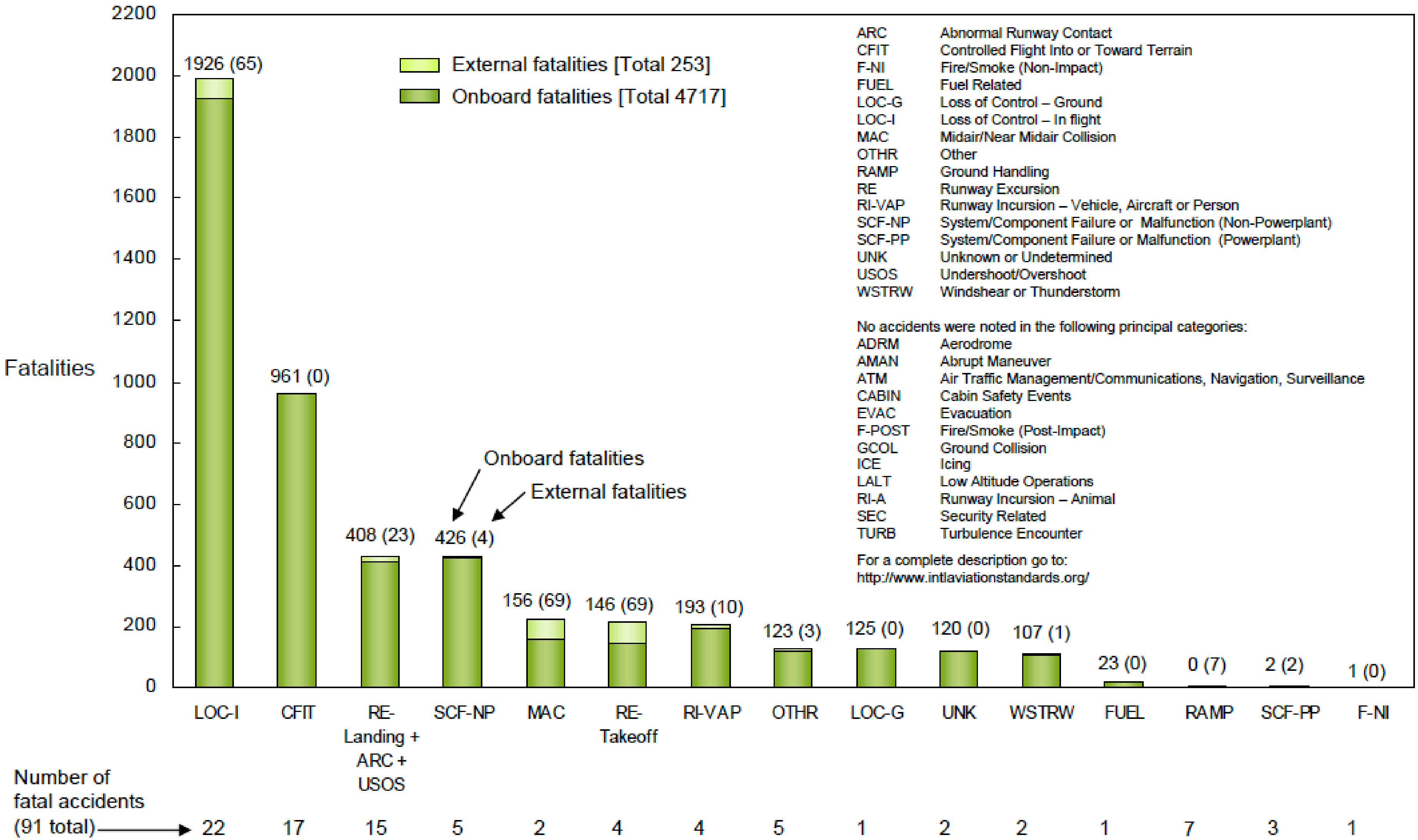
COGNITIVE ENGINEERING CENTER

Interacting With Our Community



Fatalities by CAST/ICAO Common Taxonomy Team (CICTT) Aviation Occurrence Categories

Fatal Accidents – Worldwide Commercial Jet Fleet – 1999 Through 2008



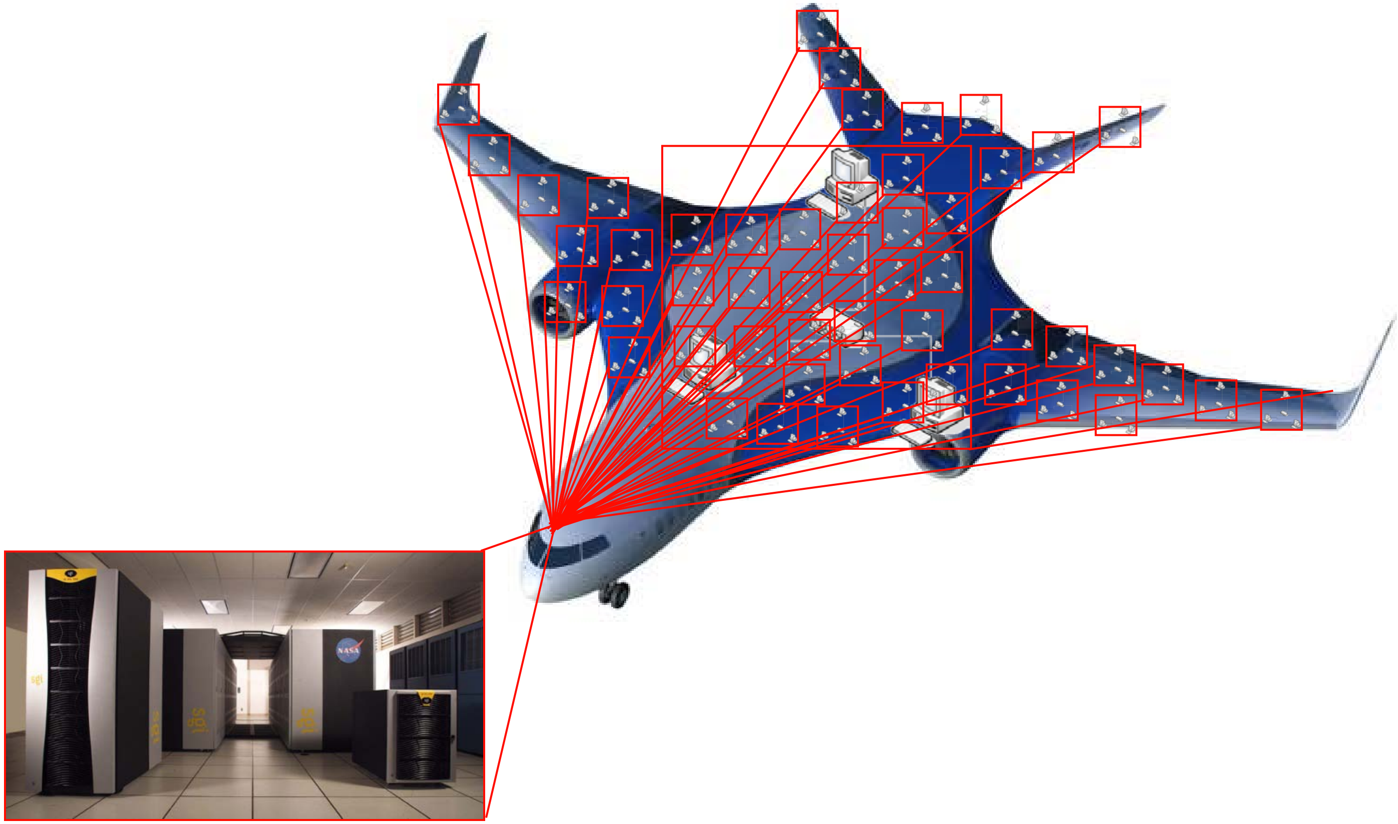
Note: Principal categories as assigned by CAST.

Note: This chart only applies to commercial aircraft weighing more than 60,000 lbs.

From Isolated Sensors -> Systems Reasoning

It’s not about the sensors alone –

It’s about making sense of them!



Monitoring and Prediction of Safety Issues from Operational Data

PROBLEM STATEMENT

- Develop data mining tools to uncover potential safety issues from massive data sources containing discrete, continuous, and textual information.
- Tools must scale to massive data sources and provide automated detection, diagnosis, and prognosis capabilities at the fleet-level.

Google easyJet

$$\text{minimize} \quad Q = \frac{1}{2}\sum_{i,j} \alpha_i \alpha_j \left(\beta K_d(x_i, x_j) + (1-\beta) K_c(x_i, x_j)\right)$$

$$\text{subject to} \quad 0 \leq \alpha_i \leq \frac{1}{\ell\nu}, \quad \nu \in [0,1], \quad \sum_i \alpha_i = 1$$

RESEARCH APPROACH

- Anomaly detection method that has the ability to detect at least three anomalies in fleet-wide heterogeneous data sources.
- Forecasting technology that has the ability to predict at least 3 known anomalies in real or emulated data of large, fleet-wide heterogeneous data sources
- Develop techniques to classify text reports into anomaly categories.

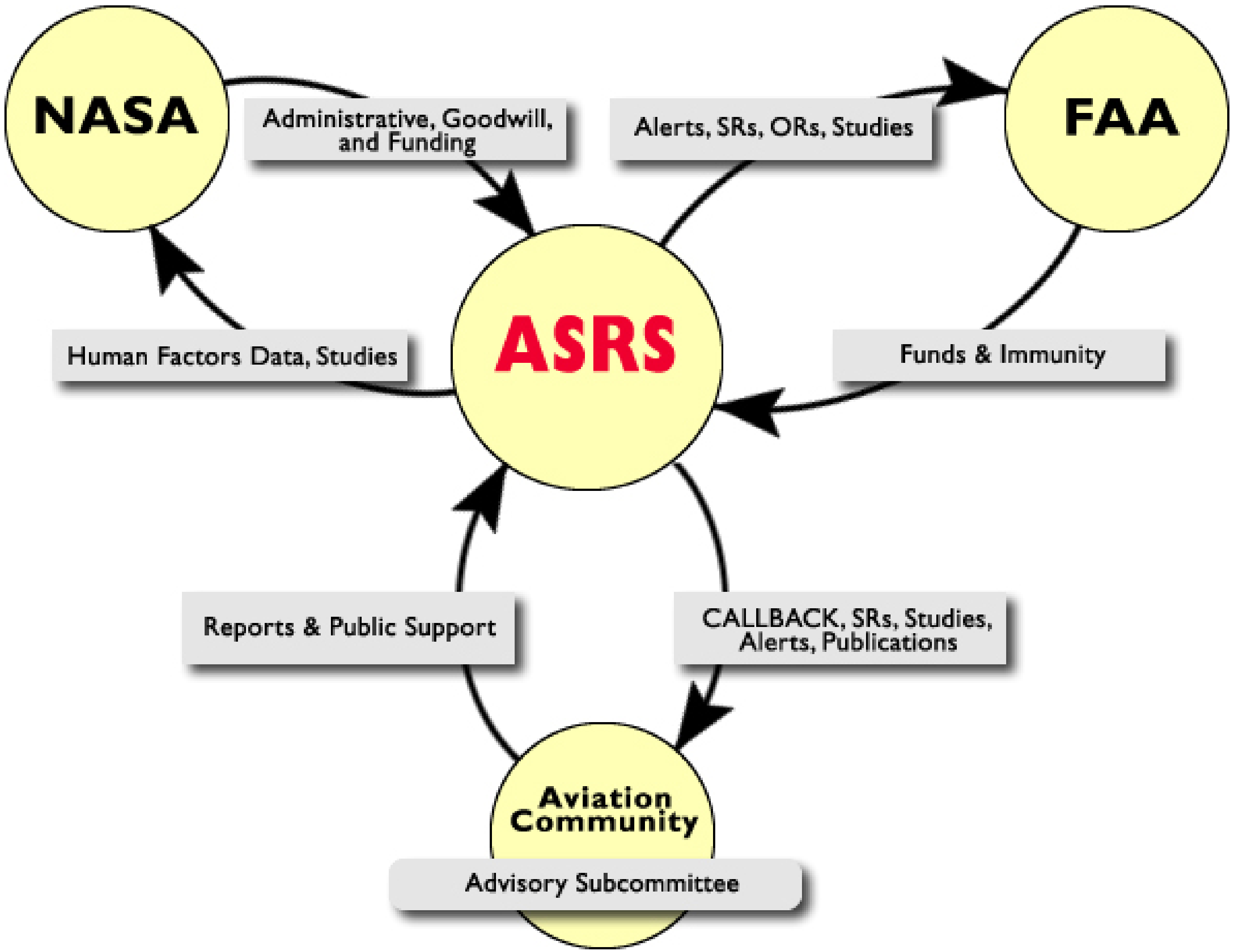
KEY MILESTONES

- **3.3.4 (FY12Q4)**: Forecasting fleet-level anomalies from massive data sources.
- **1.3.1.3 (FY10Q4)**: Anomaly detection in distributed and centralized data systems and deploy algorithms.
- **1.3.3.4 (FY011Q4):** Develop methods to predict anomalies in combined continuous and discrete sources.
- **1.3.5.1 (FY11Q4)**: Implement two prototype tools to evaluate airspace system health.

Key Policy Questions (Without Technical Insight)

+ Who 'owns' the data?
+ May the government possess it?
  - NASA (Research)
  - FAA (Regulatory)
+ If the government possesses it, can they protect it?
  - Can it fit under the 'proprietary' clause of FOIA?
+ If the government might release it, should the owner of the data release it?

Stakeholders



Confidential Safety Reporting Systems

National and International Reputation

ASRS Recognized Model for Proactive Contribution to Safety & Risk Management Process

Int'l Confidential Aviation Safety Systems (ICASS)

- Includes 12 countries modeled after ASRS

Firefighters Near Miss Reporting System

- Launched August, 2005 was modeled after ASRS
- Development Task Force includes FAA and NASA ASRS

Confidential Close Call Reporting System (C3RS)

- Railroad Safety Reporting System was modeled after ASRS
- Under development through collaboration with Federal Rail Administration, Volpe National Transportation System Center, and Railroad Industry

Patient Safety Reporting System (PSRS)

- Collaboration between NASA ASRS and Dept of VA, National Center for Patient Safety

Key Policy Questions (With Technical Insight)

+ Are there intermediate levels of analysis
  - ‘In-house’ methods on observable data
  - ‘Out-of-house’ methods for national assessment

+ Can government agencies provide standard data mining tools and protocols to data-owners?
  - Data stays ‘in-house’ with owners
  - Results of data-mining

What To Do With the Insights Gained?

+ Role of Government Research -> Industry
+ Role of the Regulator:
  - Is it possible for a government agency to maintain sufficient oversight to achieve desired safety levels?
  - Or, do we involve multiple stakeholders in private-public partnerships that collectively achieve safety?!
    - Regulator (FAA)
    - Air Traffic Operator (FAA)
    - Aircraft Operators / Air Carriers
    - Airports
    - Labor
    - Airframers & Avionics Manufacturers
    - Technical Advisor (NASA)
    - International Partners (ICAO, other CAA)

CAST brings key stakeholders to cooperatively develop & implement a prioritized safety agenda

Industry

- AIA
- Airbus
- ALPA
- APA
- ATA
- IFALPA
- NACA
- Boeing
- GE*
- RAA
- FSF
- IATA**
- AAPA**
- ATAC**
- APFA**

Commercial Aviation Safety Team (CAST)

Government

- DOD
- FAA
  - Aircraft Certification
  - Flight Standards
  - System Safety
  - Air Traffic Operations
  - Research
- NASA
- ICAO**
- JAA
- TCC
- NATCA**
- NTSB**
- EASA

* Representing P&W and RR

** Observer

2020 CAST SAFETY PLAN – WORKING SEs

(Total Plan – 65 SE; 42 Complete; 23 Underway)

SE #	Score	LOOSEC
24R2	2.4	AIR-1
30R1	0.7	ATA
34R1	1.5	ANM
39	4.0	ANM
47	1.2	ATO
53	4.2	ARA
120	0	AIA
101R1	0.10	AIA
121	3.02	ATA
125	1.06	ATA
127	0.3	AIR
129	1.72	AGC
130	6.39	AFS
131	30.35	ATA
133R1	2.73	AIA
134R1	1.73	AIA
136	0.98	ATA
159	0.27	ATO
162	0.0	AFS
163	0.39	ATA
165	0.0	AFS
169	2.34	AFS
170	0.42	AIA
172R1	0.97	AFS
175	0.0	ATA

SE #
Score
LOOSEC

ON TRACK *IN QUESTION* *LATE*

JIMDAT Score/2020 implementation level

CAST: 2008 Collier Trophy Award

In Summary

+ *Aviation* safety is the leader in safety in many domains!

+ Technology is only part of the solution – and only if carefully coordinated with policy:
  - Ability to assess safety of – and certify – new developments
  - Data protections <-> Information sharing
  - Shared construct of implementation