Streamlining Software Aspects of Certification

Program Overview & Status

Kelly Hayhurst

SSAC Technical Program Manager
NASA Langley Research Center, Mail Stop 130
Hampton, VA 23681-2199
p: 757-864-6215 f: 757-864-4234
k.j.hayhurst@larc.nasa.gov
http://shemesh.larc.nasa.gov/ssac/

Motivation for Streamlining

- There have been many *highly visible* examples of large, complex systems that have experienced significant cost and schedule overruns
  - especially true for acquisition of ground equipment for Communications, Navigation, and Surveillance for Air Traffic Management (CNS/ATM)

    "many attempts to take advantage of new CNS/ATM technologies have not produced the benefits expected and have taken far longer, and been more costly to implement, than expected." *from RTCA Task Force 4 Certification*

  - ***software development has been a chronic source of problems***

Cost and Schedule Variances for Key FAA Modernization Programs

	Estimated Total Program Cost		Scheduled Operations	
Program	**Original (in millions)**	**Current (in millions)**	**Original**	**Current**
WAAS Wide Area Augmentation System	$892.4	$2,900.0	1998	2000
STARS Standard Terminal Automation Replacement System	$940.2	$1,400.0	1998	2002
AMASS Airport Movement Area Safety System	$59.8	$151.8	1996	2002

- from *Modernizing the Federal Aviation Administration: Challenges and Solutions*, Office of the Inspector General, Report # AV-2000-039, Feb. 17, 2000

Common Problem

"What all these systems have in common are difficulties with software development and human factors.

For example, WAAS has experienced development difficulty in a critical software safety package that, among other things, determines the effects of the ionosphere on the WAAS signal and the validity of the WAAS message.

The STARS schedule has been impacted by the software development needed to resolve computer-human interface issues and other new requirements. As a result of these problems, schedules have proven to be unrealistic and costs have increased."

- from *Modernizing the Federal Aviation Administration: Challenges and Solutions*, Office of the Inspector General, Report # AV-2000-039, Feb. 17, 2000

Differences in Software Approval within the FAA

Airborne	Ground-based
• Aircraft Certification Service (AIR) deals with certification issues for airborne systems and equipment • Airborne equipment is certified – in compliance with the Federal Aviation Regulations (FARs) • FAA is only a regulator for airborne systems; i.e., the FAA does not purchase airborne equipment	• Research and Acquisitions (ARA) & Air Traffic Services (ATS) are responsible for most ground-based systems and equipment • Ground-based equipment is "commissioned" – in compliance with FAA Orders and contracts -- not FARs • FAA is both the acquirer and regulator for ground-based equipment

Software Guidance -- DO-178B

Airborne

- Complying with DO-178B is the typical means of securing approval
- Complaints by industry that compliance with DO-178B costs too much

Ground-based

- No standard means for securing approval
- Worry about cost of complying with DO-178B

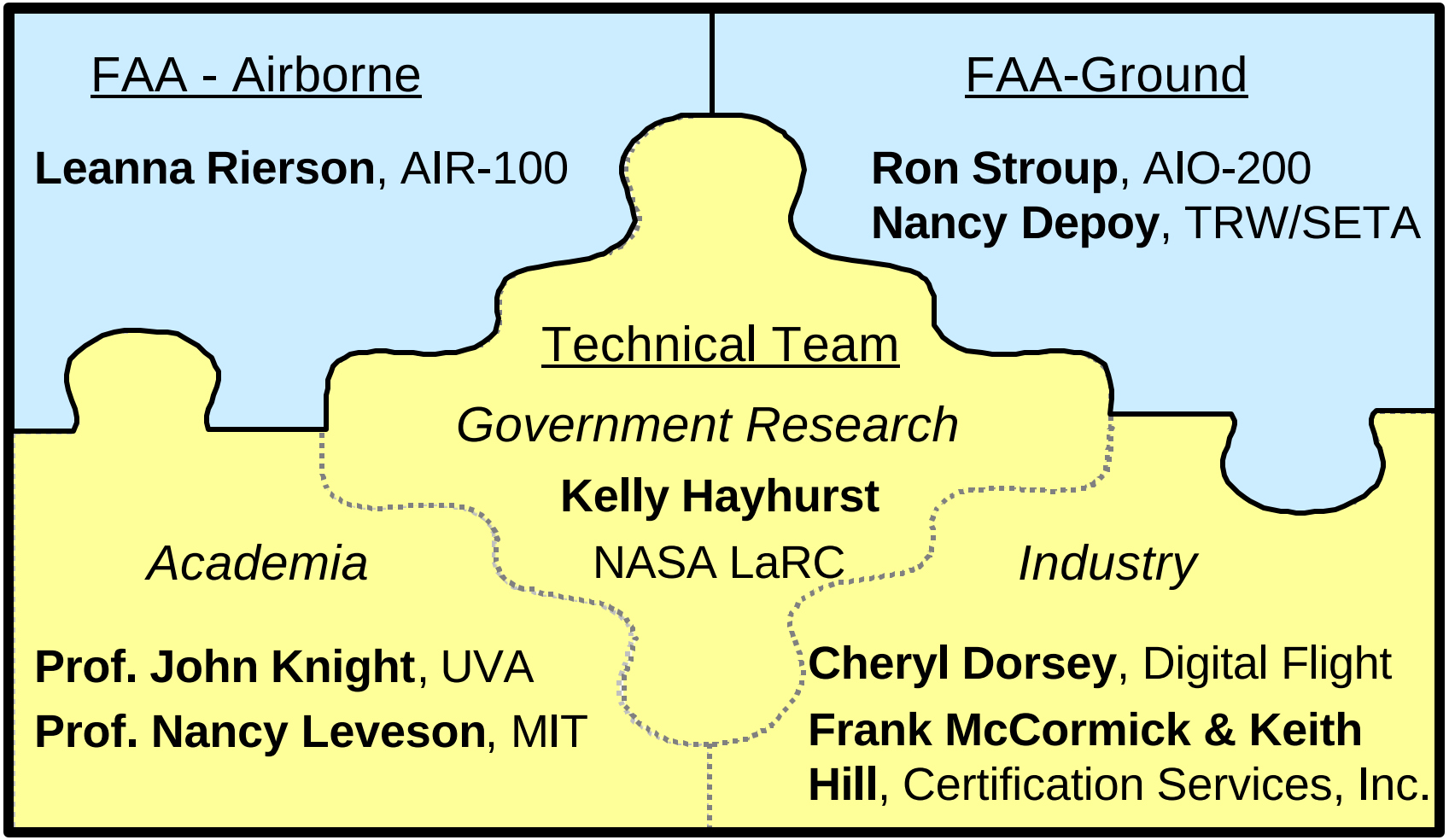
SSAC Charter

- In November 1997, the FAA commissioned an independent technical team to:

Make recommendations to the FAA to reduce the cost and time associated with software aspects of certification for both airborne and ground-based systems while maintaining or improving safety

- ***Focus on identifying non-value-added requirements in DO-178B***

SSAC Technical Team

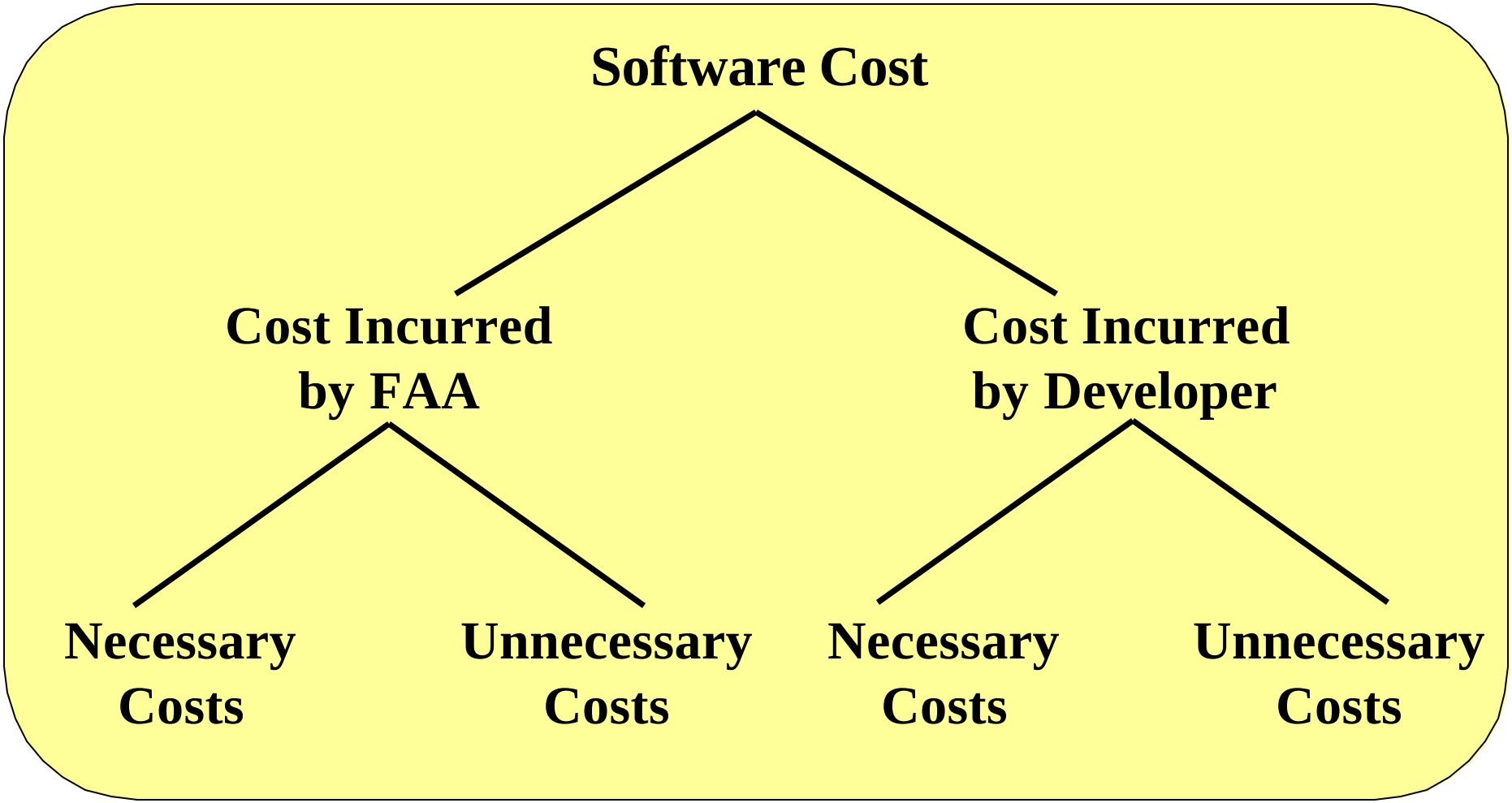


Guiding Principle

"A little data that is well understood and carefully collected, modeled, and interpreted is better than a vast amount of data without these properties."

- Manny Lehman, from *201 Principles of Software Development*

Understanding Cost and Schedule Drivers



Our Approach

- Develop a solid understanding of software cost and schedule drivers by working directly with all relevant parties:
  - software developers & regulators for both airborne & ground-based systems
- Carefully collect as much ***data*** as possible from each party
  1. identify possible cost and schedule issues through workshops
  2. prioritize issues
  3. assess extent and significance of issues through more comprehensive data collection (e.g. surveys or interviews)
- Make recommendations to the FAA based on integrated results

Getting the Developers' Perspective (airborne & ground-based)

1. Held Workshop I, January '98 with 100+ industry representatives to record their concerns with software aspects of certification
   - recorded over 200 individual issues
2. Determined which issues were considered most important at Workshop II, May '98
   - also started to draft guidance in areas with clear needs
     - major/minor software changes
     - tool qualification
     - reuse of certification data
     - best practices for FAA and industry

Top 10 Industry Issues

1. Inconsistencies exist among ACOs in interpreting and following policy and guidance.
2. The effectiveness of some specific activities required by DO-178B is unclear.
3. DO-178B inadequately addresses the effect of software on the safety of the overall system.
4. Insufficient knowledge of software engineering and related disciplines exists within the FAA.
5. Requirements definition is difficult independent of certification.
6. Lack of cooperation exists between the FAA and industry.
7. The extent to which DO-178B provides benefits beyond those that are provided by other industry accepted practices is unclear.
8. Insufficient knowledge of software engineering and related disciplines exists within industry.
9. Insufficient information is available about the certification process.
10. Inadequacies, inconsistencies, and inefficiencies exist in the DER system.

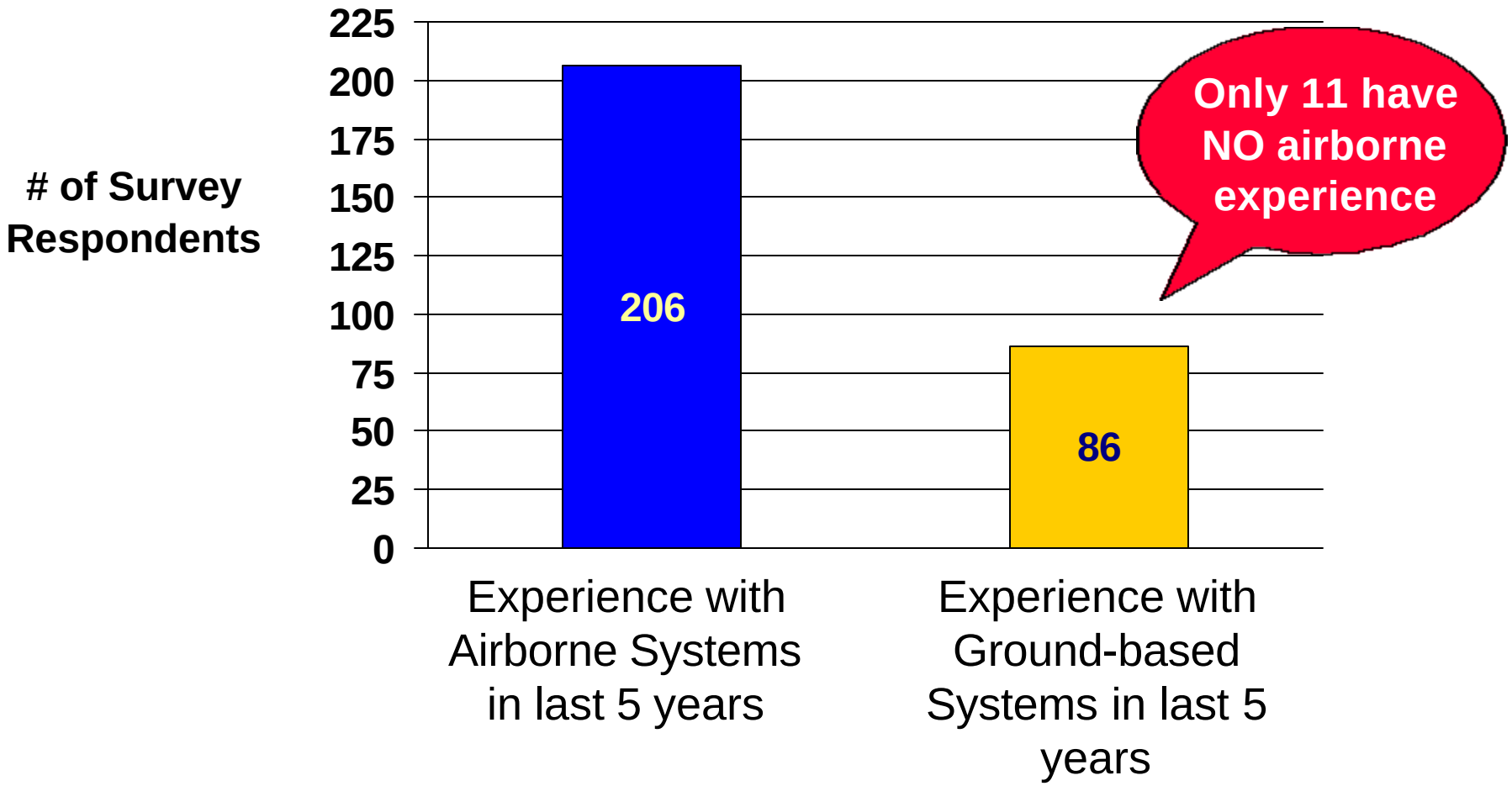
Assessing Developers' Issues

3 Conducted an industry-wide survey Dec. '98 - Feb. '99 to assess extent and significance of the priority issues

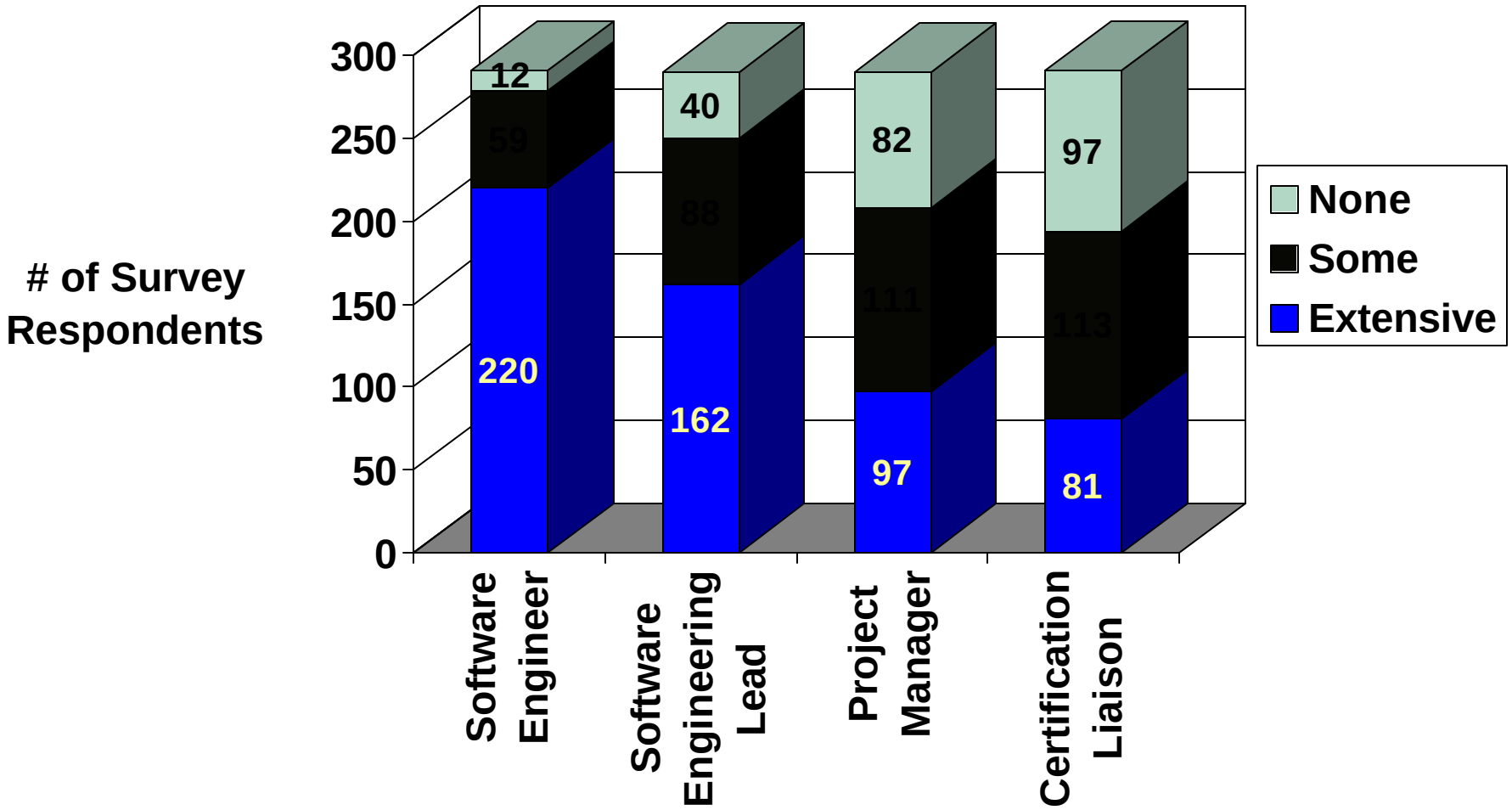
- survey contained 240+ questions addressing the top issues
- 416 surveys were distributed to 70+ companies
  - engineers & managers
  - airborne & ground-based systems developers
  - aircraft & engine manufacturers

  } All with different levels of experience with DO-178B
- 300 surveys were returned -- for a 72% response rate
  - 292 were completed surveys suitable for analysis
- survey participants were a fair representation of the general population of aviation software developers using DO-178B

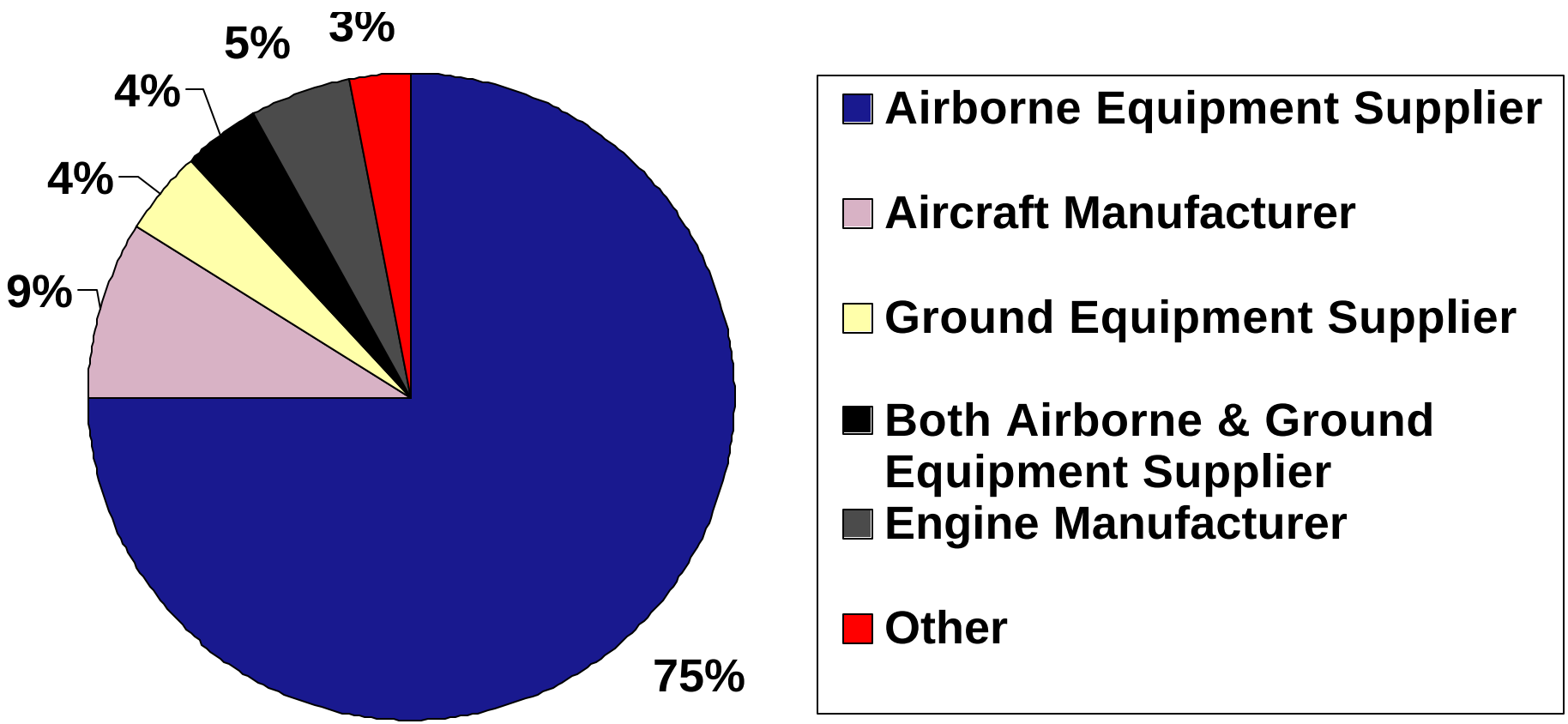
Respondent Profile: Airborne versus Ground



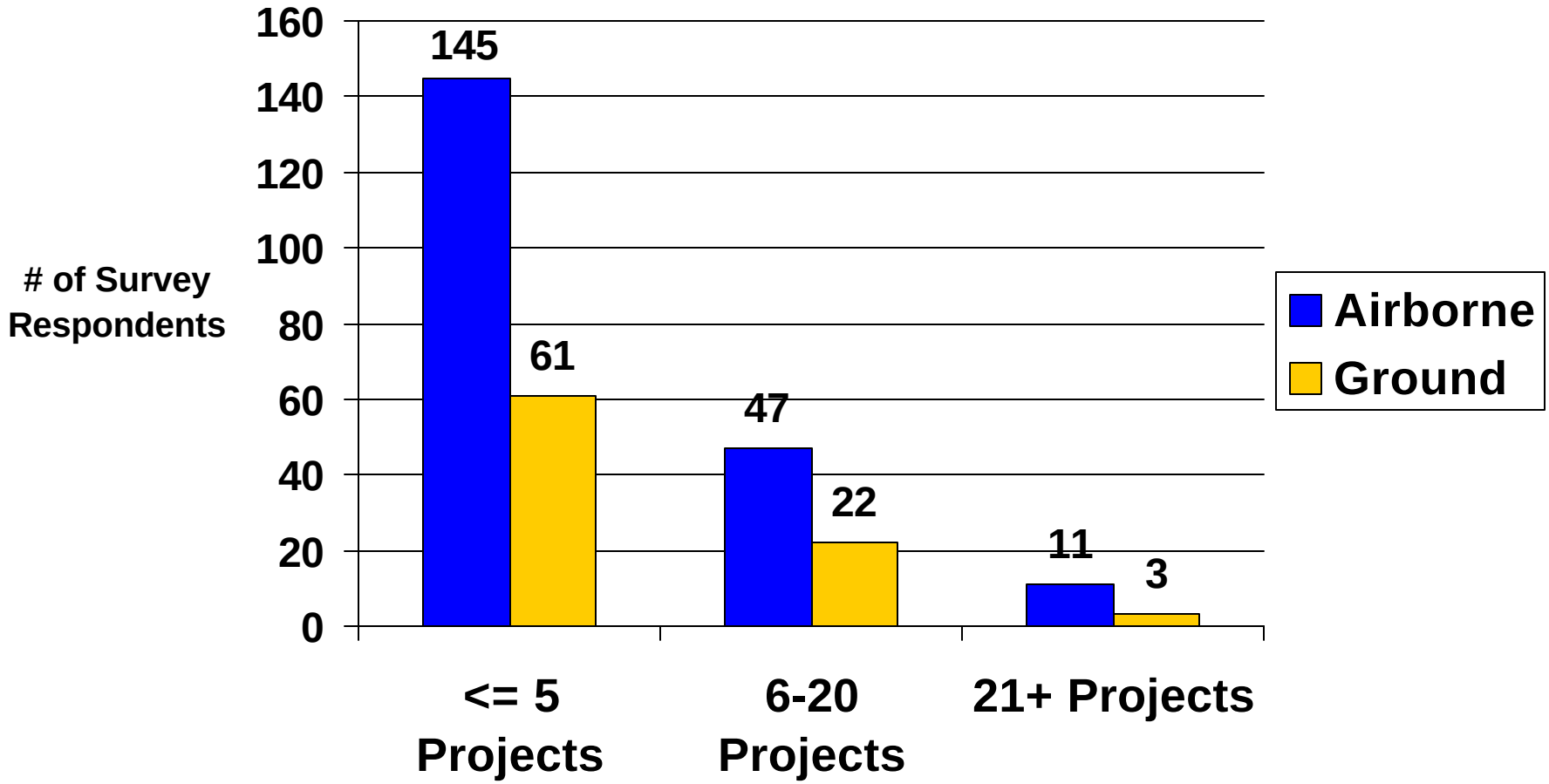
Respondent Profile: Level of Experience in Software Role



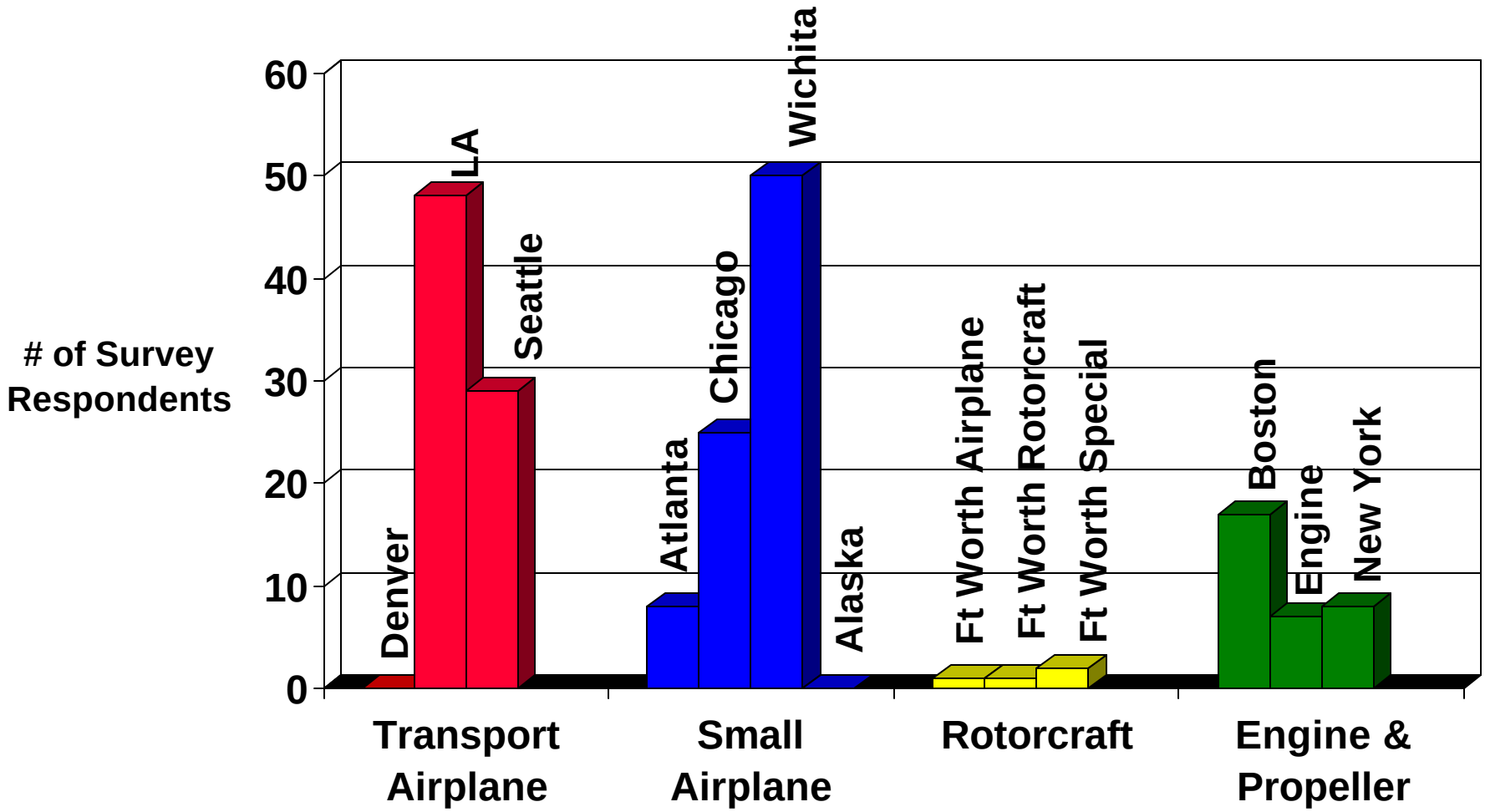
Respondent Profile: Company Type



Respondent Profile: Experience with DO-178B



Respondent Profile (airborne): Distribution by ACO



Issues Covered in the Industry Survey

Issue	Results
Inconsistencies between & within approving authorities (air & ground) in interpretation of software policy, guidance, and procedures	
Inadequacies in software policy & guidance	
Ineffectiveness of specific activities in DO-178B: - independence does not add value - MC/DC does not add value (i.e., find errors) - quality assurance does not add value - traceability does not add value - unreasonable requests for documentation - tool qualification does not add value (i.e., find errors)	
Connection between DO-178B and safety	
Inadequacies in the DER system	

Inconsistencies

Determine if there have been instances of inconsistencies
- Are there more than isolated occurrences?
- Do they impact cost & schedule?

Airborne: All ACOs

Is there inconsistency between ACOs?

76% say *yes*
> 87% occasionally+
> 61% major cost

Is there inconsistency within individual ACOs?

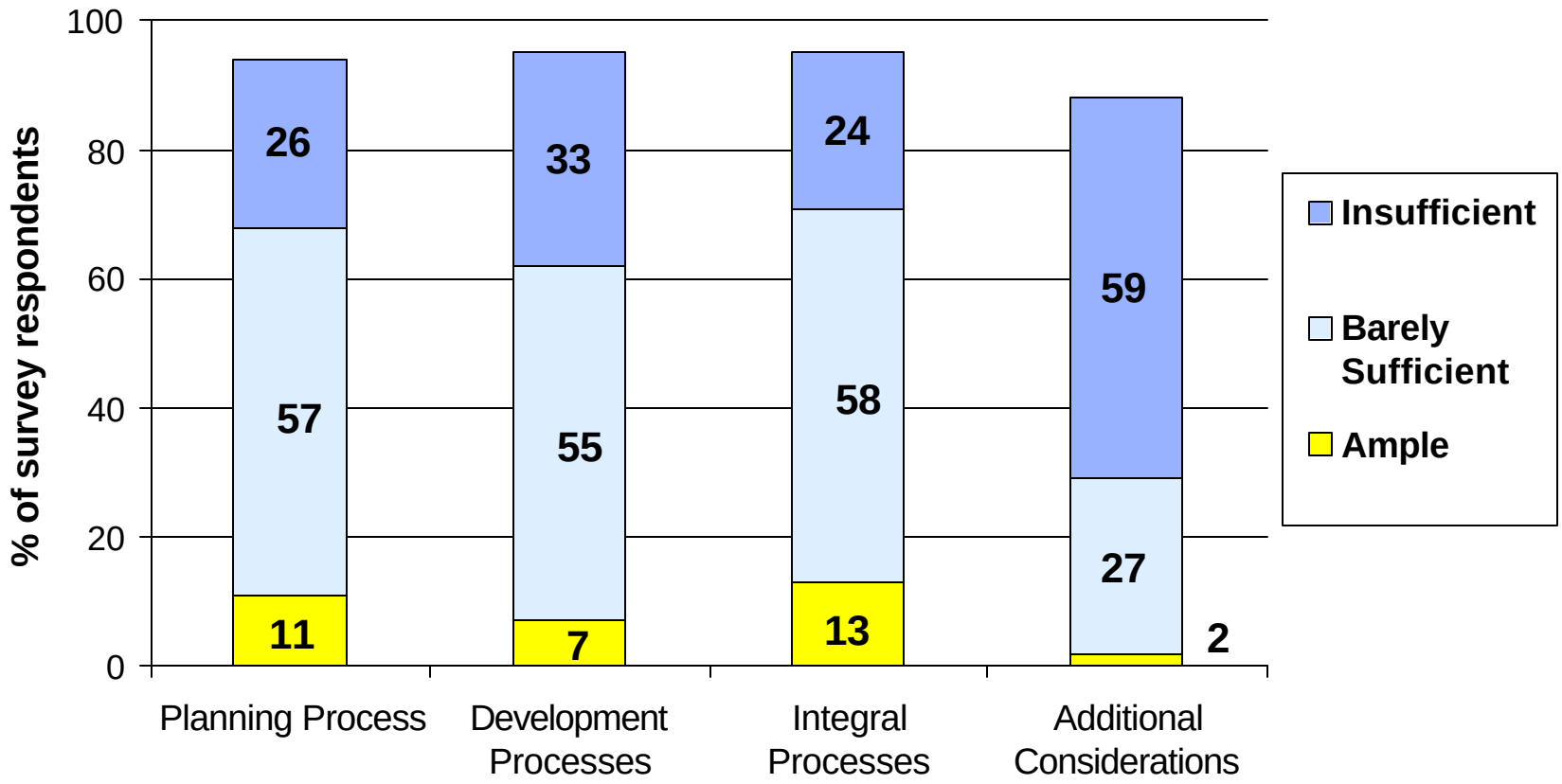
36% say *yes*
> 70% occasionally+
> 57% major cost

Ground: AND and AOS

Is there inconsistency between ground-based approving authorities?
**Only 3 have worked with both -- but all 3 report inconsistencies*

#1 Inconsistency: Interpretation of DO-178B

Satisfaction with Specific Areas of Software Policy & Guidance



- *Survey responses indicated that software policy and guidance is inadequate in both availability and quality*

Effectiveness of DO-178B Activities

- The survey asked questions to determine:
  - Is each activity understood?
  - If so, is it valuable?
  - Does it cost a lot?
- The survey results indicated:

Activities that ARE effective

Independence

Traceability

Quality Assurance

Tool Qualification

Problem Areas

MC/DC

Documentation

Activities That Are Effective

- **Independence**: requirements considered *extremely* or *somewhat valuable* by 82% of respondents
- **Traceability**: generally used effectively for requirements coverage, regression analysis, and change impact analysis
  - but, cost and time are *substantial*
- **SQA**: objectives were considered *somewhat* or *extremely valuable* by most
  - compliance with plans (79%), transition criteria (57%), and conformity review (72%)
- **Tool Qualification**: Errors have been found during tool qualification while cost is *negligible* to *small*
  - 44% found an error in a development tool
  - 57% found an error in a verification tool

Concerns about MC/DC

- 79% say MC/DC is *moderately* or *extremely difficult*

  21% say MC/DC is *moderately* or *trivially simple*

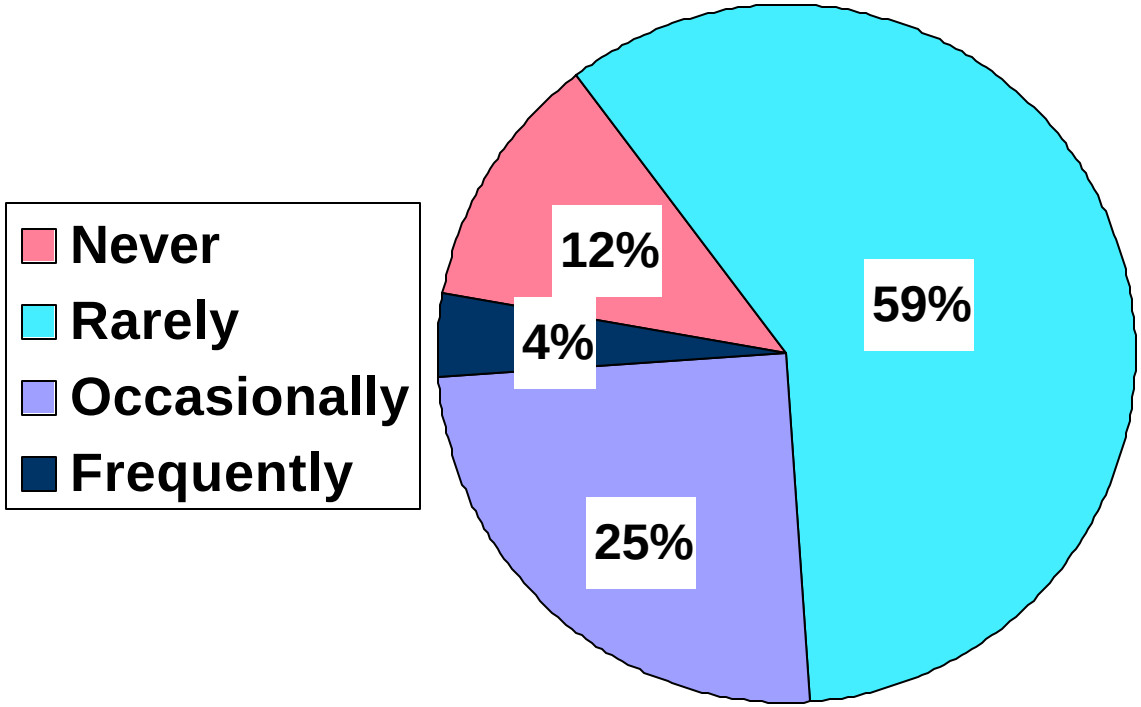
- Different approaches are used:
  - 59% do requirements-based testing with additional tests to meet structural coverage
  - 33% do structural testing independent of requirements-based testing

- 75% say that cost and time for MC/DC are *substantial* or *nearly prohibitive*

A significant number of respondents report finding errors with MC/DC

MC/DC -- Effectiveness

Frequency with which errors have been found with MC/DC



- Of those who have found errors:

  21 said they have found safety-critical errors

Concerns about Documentation

- Most concerns were about submitting certification data

Has the FAA made requests for ...

data/documentation that is not required by DO-178B or the FARs?	data/documentation to meet certification requirements that is used for nothing else?	documentation at the end of the project that had no impact on safety and maintenance?
Yes 34%	**Yes 40%**	**Yes 55%**
No 66 %	**No 60%**	**No 45%**

- Examples cited by the respondents indicated misunderstandings about certification data

Safety

Things that were clear from the survey data:

- 28% report working on a system that had a software-related system error resulting in a service bulletin or AD
  - requirements were cited as the most frequent source of error
- Derived requirements are handled in different ways
  - 9% report handling derived requirements as per DO-178B
  - 23% report that derived requirements have led to safety-related mods to system design

Things that were not clear from the survey data:

- Connection between DO-178B and safety
  - respondents reported they do "additional activities outside of those required by DO-178B for software-related safety issues"
    - some of these were related to ARP-4754 and ARP-4761
- How much of the information from these system activities is used during software development

Satisfaction with the DER System

- On the **airborne side**, satisfaction is high -- except for training

Satisfaction with...		
primary software DER:	**somewhat or very satisfied**	**80%**
	somewhat or very dissatisfied	**10%**
degree of delegation:	**about right**	**70%**
	too much given to DERs	**5%**
FAA training of DERs:	**inadequate**	**43.5%**
	adequate	**56.5%**

- On the **ground side**, of the 30 respondents who have worked with a software DER
  - 80+% report improved ability to work with DO-178B and reduced delay in approval of submissions
  - 73% agree that FAA should expand the authority of software DERs for ground-based systems

Summary of Issues

Issue	Results
Inconsistencies between & within approving authorities (air & ground) in interpretation of software policy, guidance, and procedures	Validated
Inadequacies in software policy & guidance	Validated
Ineffectiveness of specific activities in DO-178B:	
- independence does not add value	Refuted
- MCDC does not add value/find errors	Refuted
- quality assurance does not add value	Refuted
- traceability does not add value	Refuted
- unreasonable requests for documentation	Validated
- tool qualification does not add value/find errors	Refuted
Connection between DO-178B and safety	More data needed
Inadequacies in the DER system	Validated

Getting the Regulators' Perspective

FAA-Airborne

- Conduct workshop to identify & prioritize issues
- Conduct survey to determine the extent and significance of the issues for FAA-Airborne population in general

FAA-Ground

- Document current assurance practices for development
- Identify consistencies and inconsistencies among the Integrated Product Teams

Combine with data from industry survey & make recommendations as necessary

FAA-Airborne Perspective

1. Held a Workshop, October '99 with FAA officials from 13 different organizations responsible for **airborne** systems containing software
   - recorded 132 individual issues
2. Determined which issues were considered most important
   - had workshop attendees vote on top issues (by email after workshop)
3. Planned to conduct a survey of all FAA employees responsible for software aspects of certification for airborne systems
   - *funding difficulties prevented realizing this plan*

Top Issues for FAA-Airborne

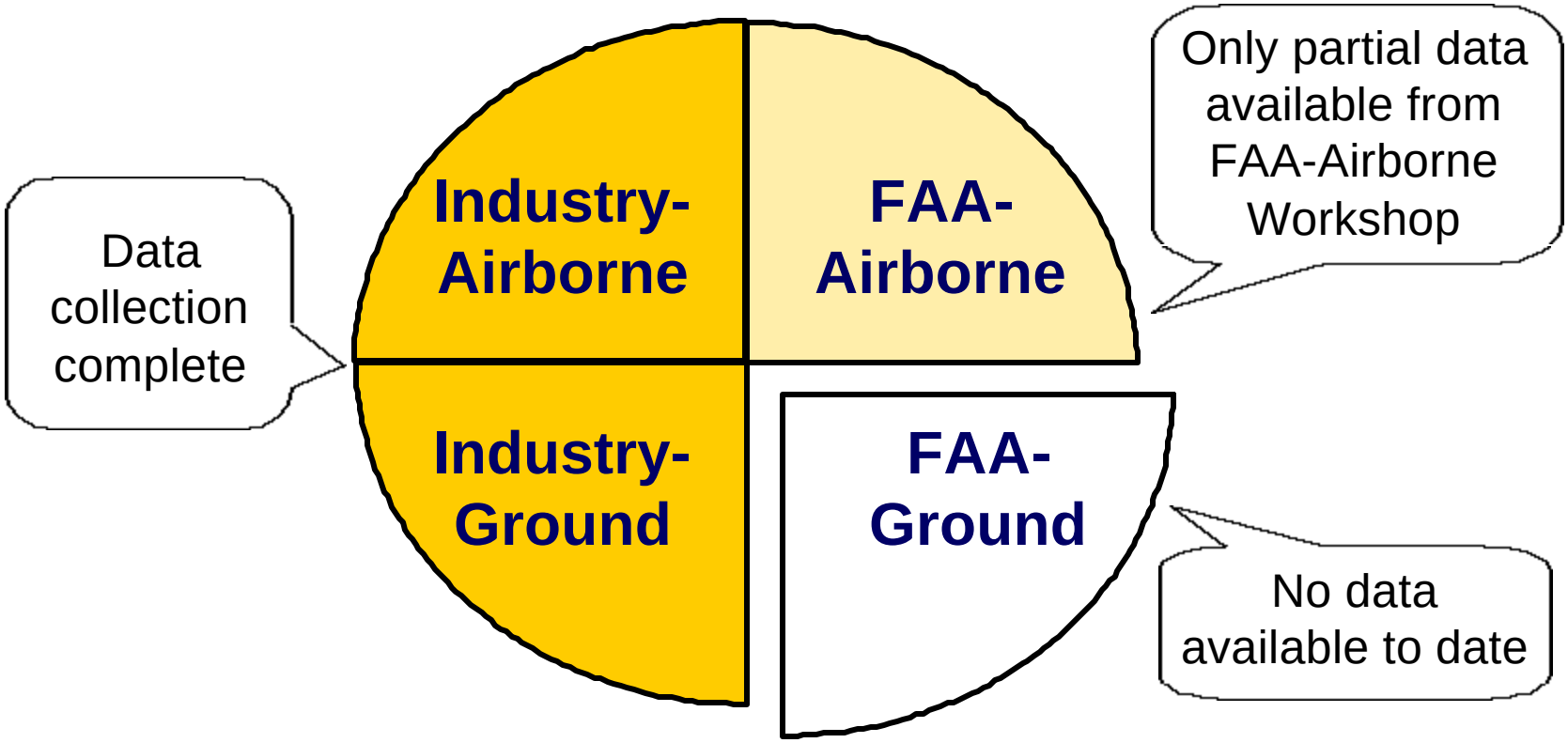
- Top issues were determined by a very small sample of the FAA
  - issues won't be made public until substantiated through more extensive data collection
- Some of the FAA-Airborne issues overlap with Industry Issues
- Some of the FAA-Airborne issues are new issues
  - *further data collection from within the FAA would be valuable*

FAA-Ground Perspective

Direction: Consistent assurance processes for software aspects of airborne and ground-based systems

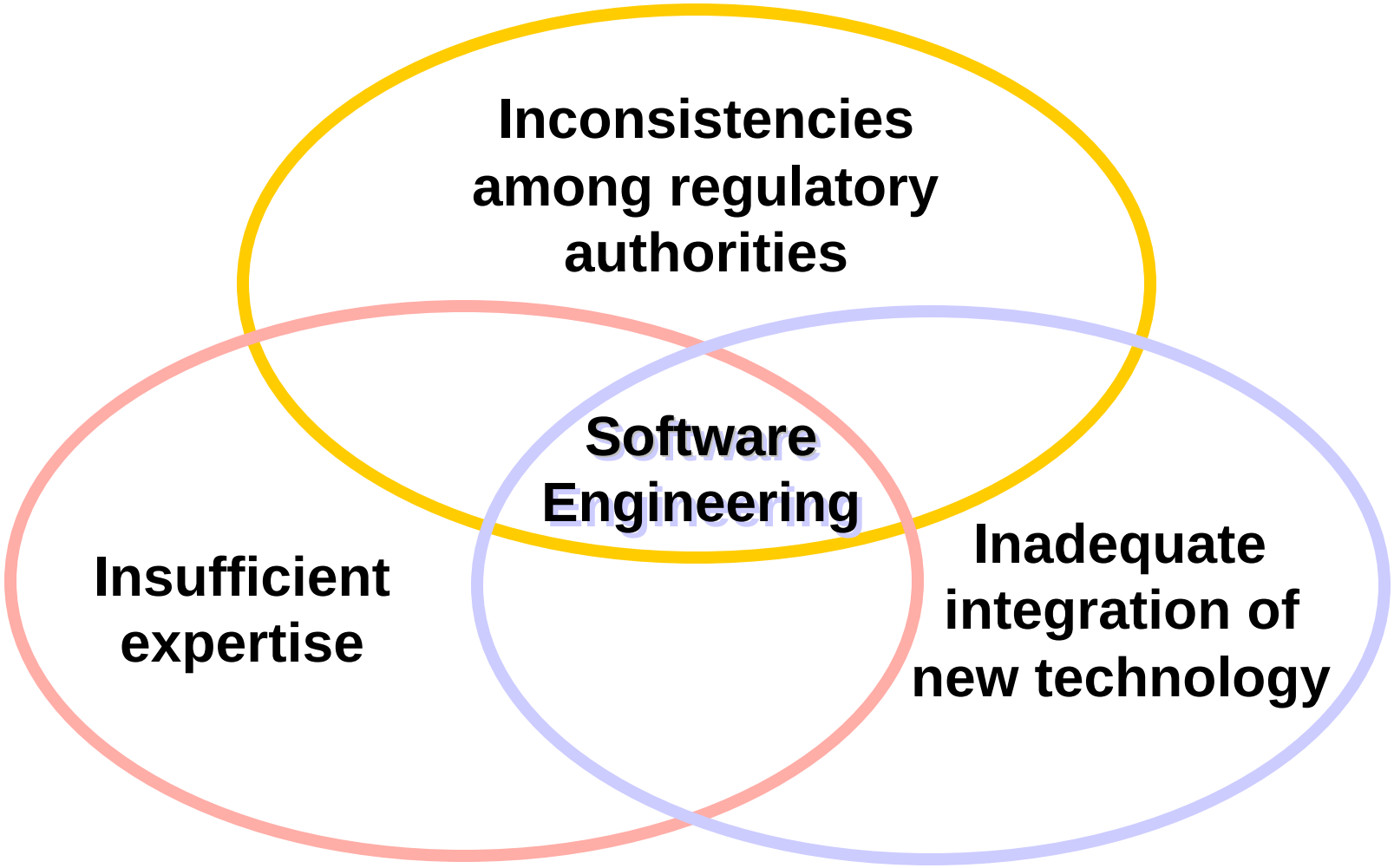
- Procurement, development, approval, deployment, and maintenance are undertaken by different entities for different ground-based systems
  - so, there is no singular ground perspective
- Difference in approaches within the ground community may be a potential source for reducing certification costs
- However, the scope of activities make data collection difficult and time-consuming

Status of Data Collection



- From this data, the SSAC technical team made
  - low-level recommendations for each subject area in the survey
  - a set of general observations
  - 10 high-level recommendations

General Observations
(based on available data)



Observations about Inconsistencies

FAA authorities create unnecessary cost burdens (for both industry & the FAA) through inconsistent guidance, interpretation, and procedural requirements for software-related issues.

- **inconsistencies between the airborne and ground-based software approval processes**
- **inconsistencies among Aircraft Certification Offices and other approving authorities**
- **inconsistencies within individual offices**

Observations about Expertise

The FAA has not allocated enough people with the requisite software engineering expertise and knowledge of DO-178B to software approval issues.

Knowledge of and experience with DO-178B and other certification policy and processes vary substantially among software developers.

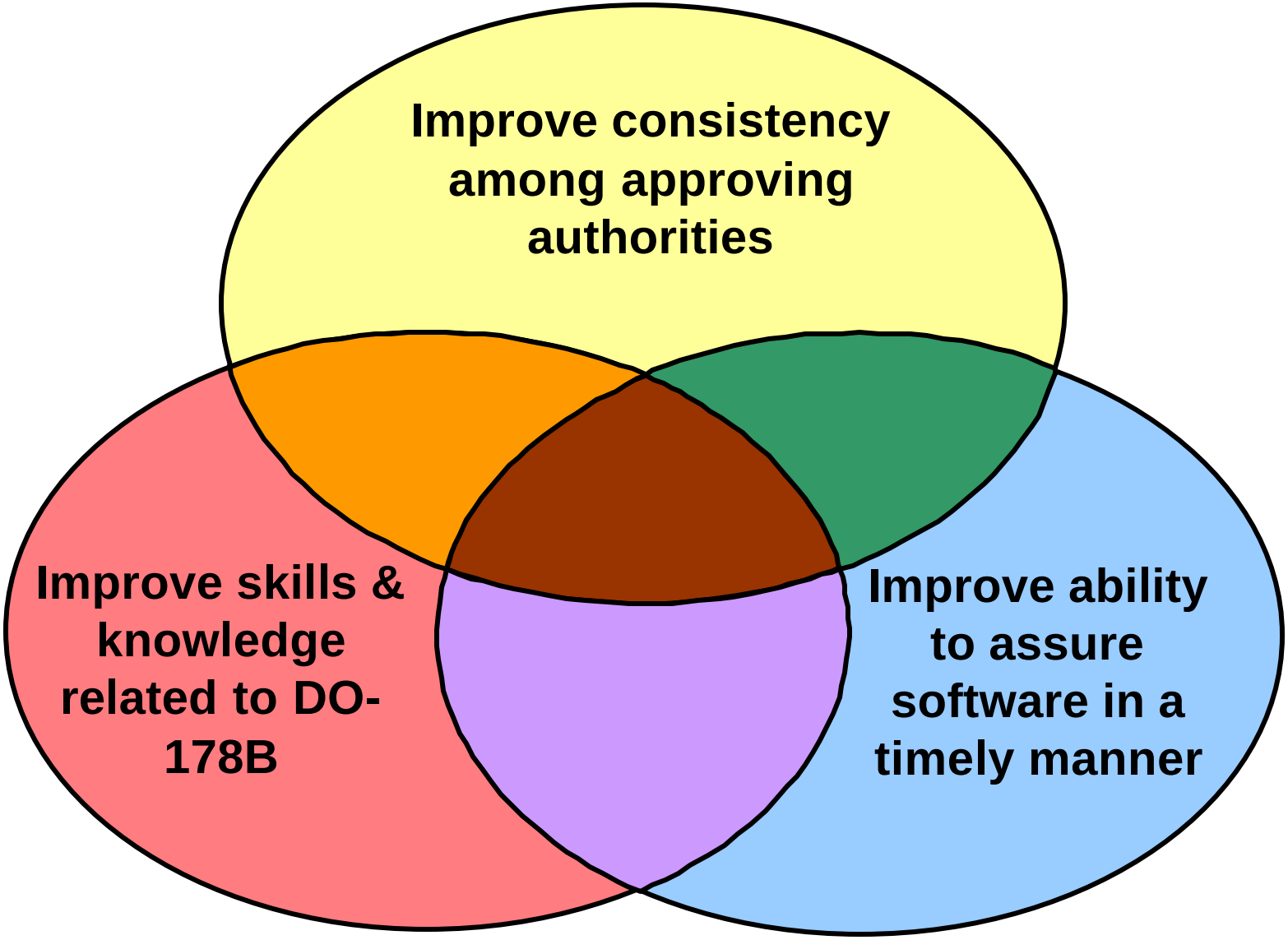
Definition and flow of requirements at all levels (system, high, low, and derived) is difficult independent of certification.

Observations about Integration

The FAA is not keeping pace with software technology, thereby delaying the use of potentially cost saving technology.

Software issues exist for which FAA software policy or guidance is inadequate.

High-Level Recommendations



Recommendations to Improve Consistency

- **The FAA should determine the causes for inconsistencies between and within approving authorities for both airborne and ground-based systems, and determine what, if any actions, are required in addition to those recommended.**
- **The FAA should develop unified policy and guidance for approving software aspects of airborne and ground-based systems.**
- **The FAA should institute a regulatory authority independent of acquisition authority for approval of ground-based systems.**

Recommendations to Improve Skills & Knowledge Within FAA

- **The FAA should hire a sufficient number of software engineering experts to understand the safety impact of software technologies for both airborne and ground-based systems.**
- **The FAA should improve software expertise by:**
  - **identifying the minimum staffing needed to assure a consistent approach and timely response for software approvals**
  - **continually assessing software personnel needs and hiring to meet those needs**
  - **creating, funding, and filling software engineering positions**
  - **requiring software engineers who appoint and advise designees to meet the same qualifications as the designees**

Recommendations to Improve Skills & Knowledge Within Industry

- **The FAA should require companies providing software for airborne or ground-based systems to demonstrate acceptable competence in DO-178B.**

  The FAA should use DO-178B capability as a factor in establishing level of involvement in software assessment activities.

- **The FAA should make DO-178B training available to designees.**

Recommendations to Improve Ability to Assure Software

- **The FAA should establish processes for**
  - **regularly assessing software policy and guidance needs;**
  - **developing new software policy and guidance when needed; and**
  - **assessing and enhancing the clarity, consistency, and completeness of software policy and guidance.**
- **The FAA should establish a means to ensure that the software approval process allows applicants to use appropriate new software technologies in a timely manner.**

Recommendations to Improve Ability to Assure Software

- **The FAA should initiate a program of proactive research to evaluate the potential impact of software technology on cost and safety.**

  The research output should influence the development of policy, guidance, regulations, and training for software engineering.

Comparison with Other Efforts

- SSAC observations are consistent with previous government reports
  - 1993 Government Accounting Office (GAO) report GAO/RCED-93-155, *Aircraft Certification. New FAA Approach Needed to Meet Challenges of Advanced Technology*.
  - 1999 Office of the Inspector General (OIG) report *Air Traffic Control Modernization*, Report Number AV-1999-065
- SSAC observations and recommendations are consistent with those from the *Final Report of RTCA Task Force 4 Certification*, e.g.
  - poor communication between authorities' offices and particularly across organizational boundaries within an authority
  - inability to quickly update rules & standards in response to changing technology

Comparison with Other Efforts

- SSAC observations parallel many of the concerns raised in Aviation Week & Space Technology's "Air Travel in Crisis" issue, October 25, 1999
  - poor communications between facilities
  - a lack of standardized traffic management equipment, automation, and training
  - a general failure to train controllers and air traffic management personnel for working in a national system

    - from *Welcome to Gridlock, All Flights Delayed*, by James Ott, Aviation Week & Space Technology, 9/25/99

Has the SSAC Mission Been Accomplished?

SSAC Charter

Make recommendations to the FAA to reduce the cost and time associated with software aspects of certification for both airborne and ground-based systems while maintaining or improving safety

- SSAC results have been presented to several FAA organizations, including AIR, ARA, and ATS
- Full SSAC technical team activities ceased in October ‘99
  - individual team members may work on specific projects as called on by the FAA

Has SSAC Made a Difference?

"The air transportation system is showing ominous signs of a crisis--one that could have been averted if governments had responded to their own clear warnings of infrastructure inadequacies."

- from *Welcome to Gridlock, All Flights Delayed*, by James Ott, Aviation Week & Space Technology, 9/25/99

Through the SSAC program, aviation software developers were given a means to voice their concerns and work with the FAA on solutions