

Streamlining Software Aspects of Certification

Survey Findings & Preliminary Recommendations

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/>



Outline

- Survey Statistics & Profile of Survey Respondents
- Survey Findings
 - Interactions with ACOs & other approving authorities
 - Software policy & guidance
 - Effectiveness of specific activities in DO-178B
 - independence - documentation
 - MCDC - quality assurance
 - traceability - tool qualification
 - Safety
 - DER system
- General Observations
- Recommendations to the FAA



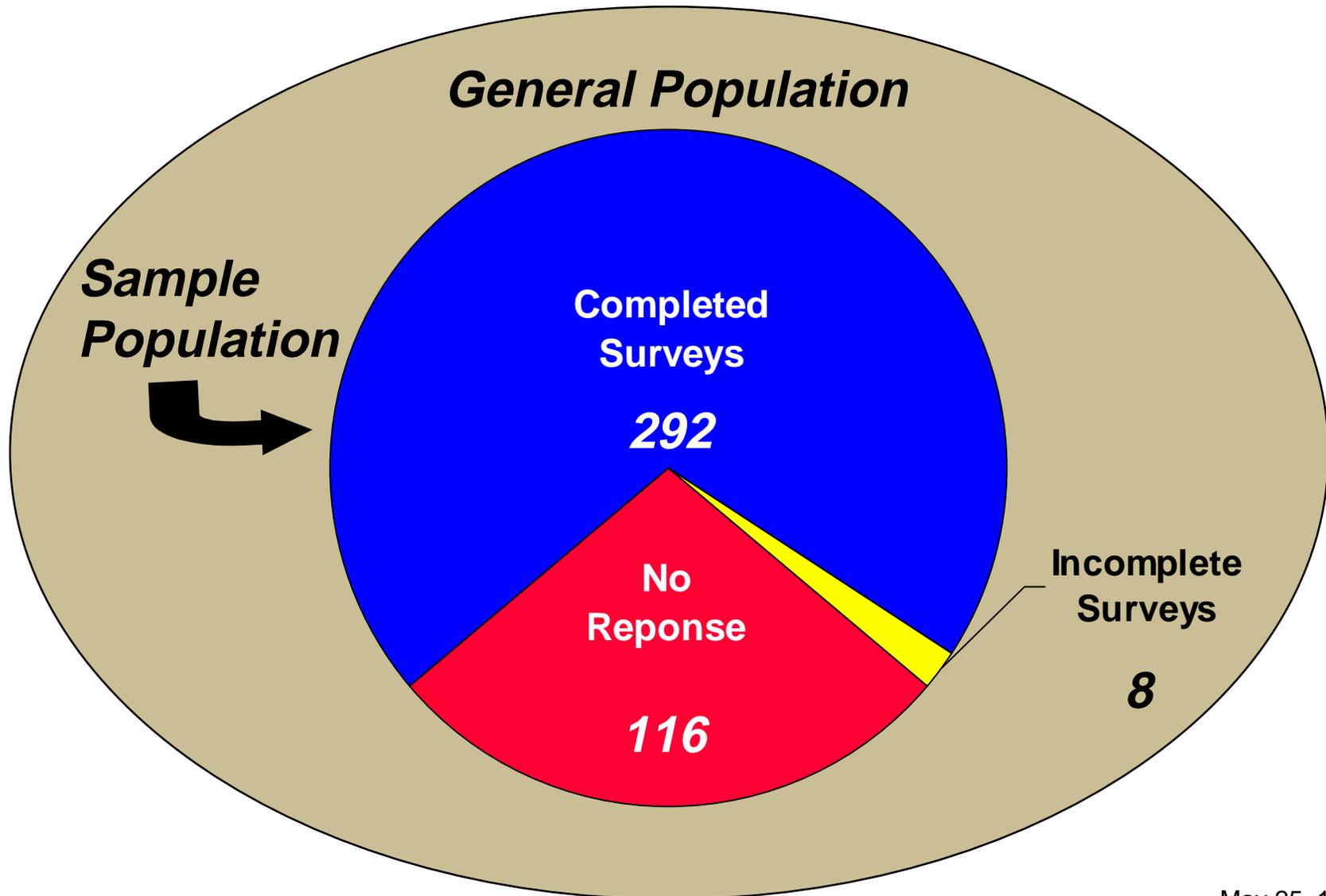
Survey Population

Survey respondents must have ...

- participated in at least 1 software development project using DO-178B
- experience in at least 1 of the following roles:
 - ◆ software engineer: responsible for software design, verification, or quality assurance
 - ◆ software engineering lead: responsible for directing software professionals
 - ◆ project manager: responsible for the overall cost and schedule including software
 - ◆ certification liaison: responsible for coordination with the Aircraft Certification Office or other approving authority. This includes but is not limited to company or consultant DERs.



Survey Statistics





Attributes of the General Population

Individual Attributes

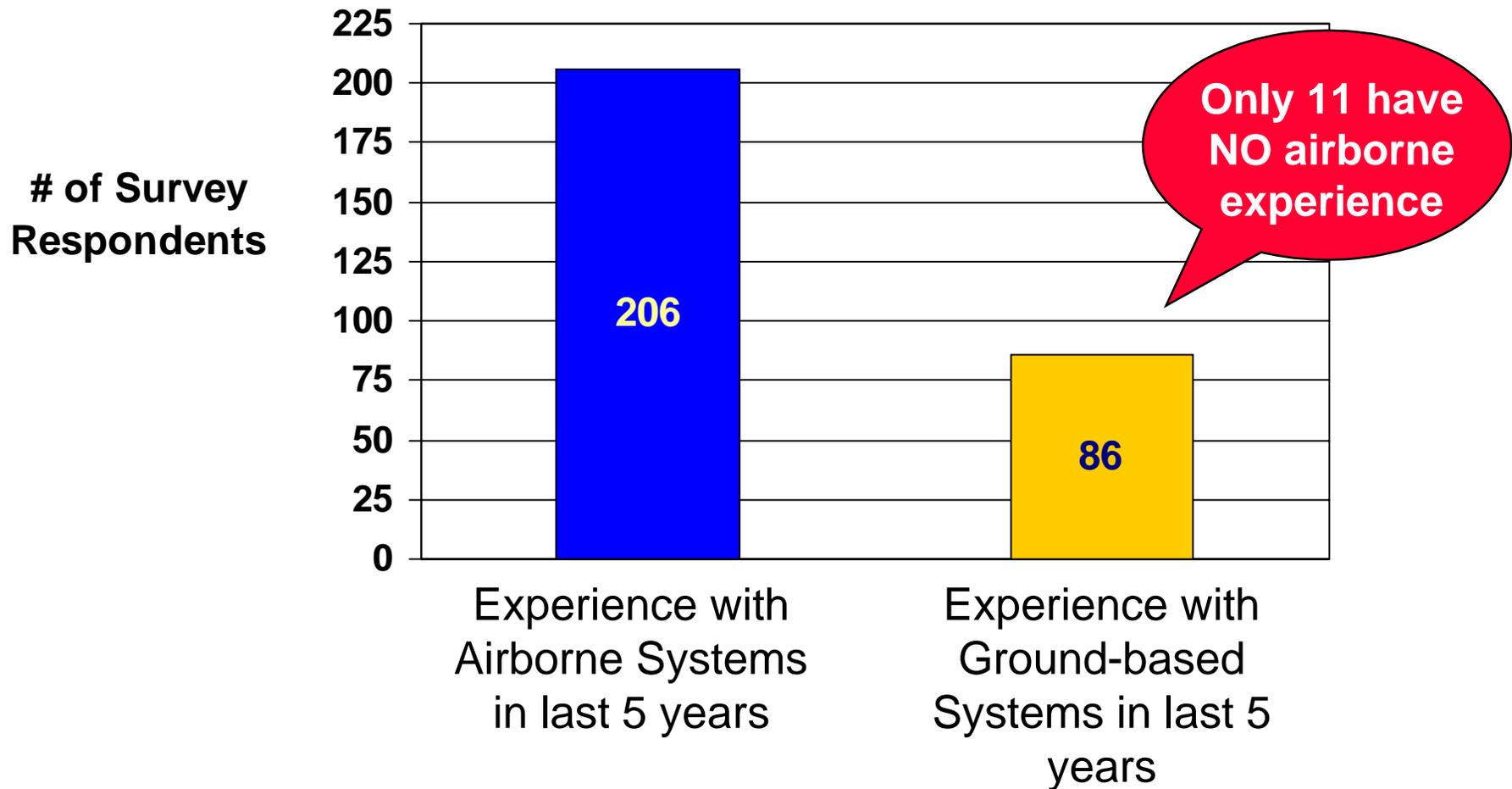
- **Experience in aviation software**
 - airborne or ground products?
- **Experience with DO-178B**
- **Employment experience**
- **Role in software development**
 - software engineer
 - software engineering lead
 - project manager
 - certification liaison

Company Attributes

- **Size**
 - team size
 - product size
- **Number of DO-178B projects**
- **Product Area**
 - airborne, ground, engine
- **Product Types**
- **Geographic Location**
- **Capability Maturity Model Level**

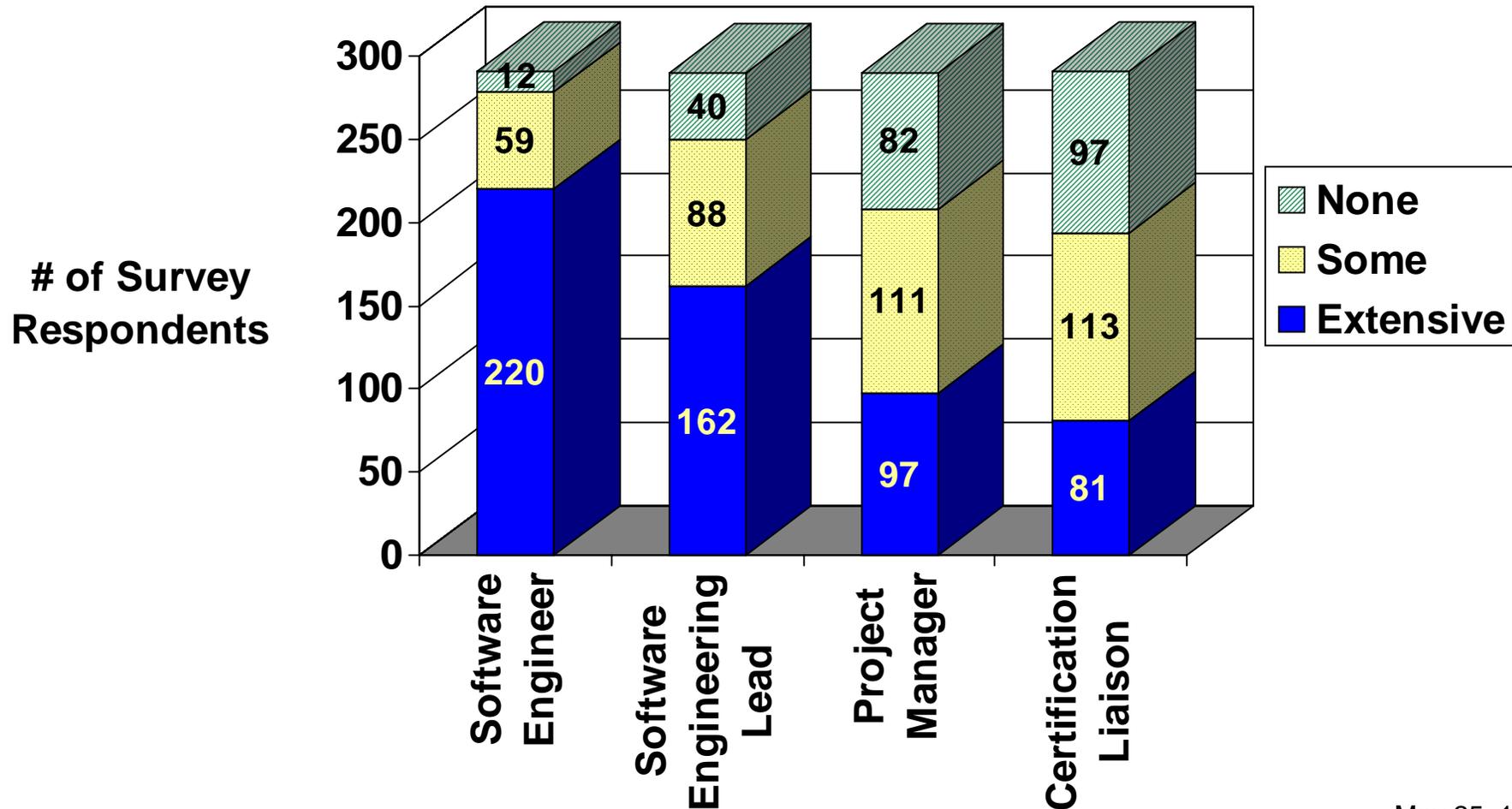


Respondent Profile: Airborne versus Ground



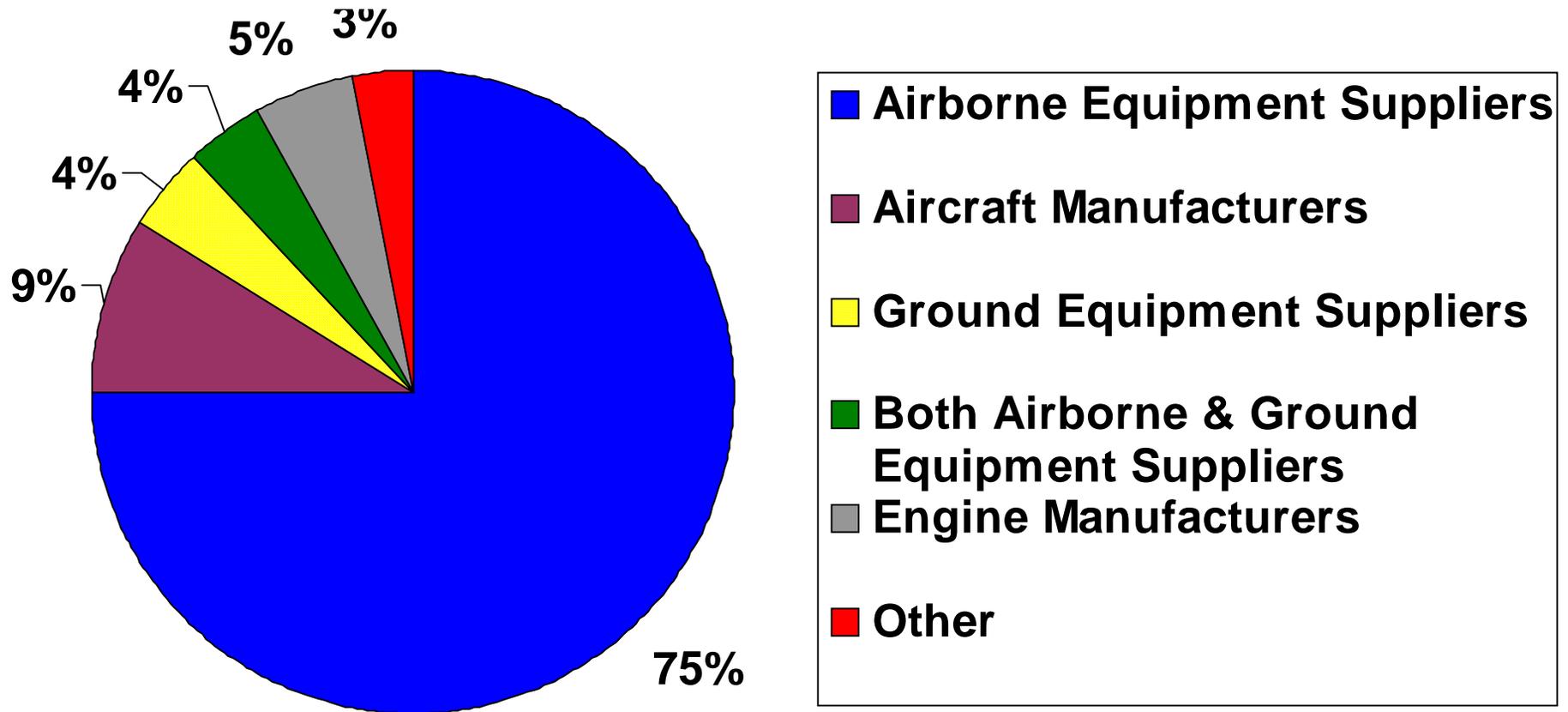


Respondent Profile: Level of Experience in Software Role



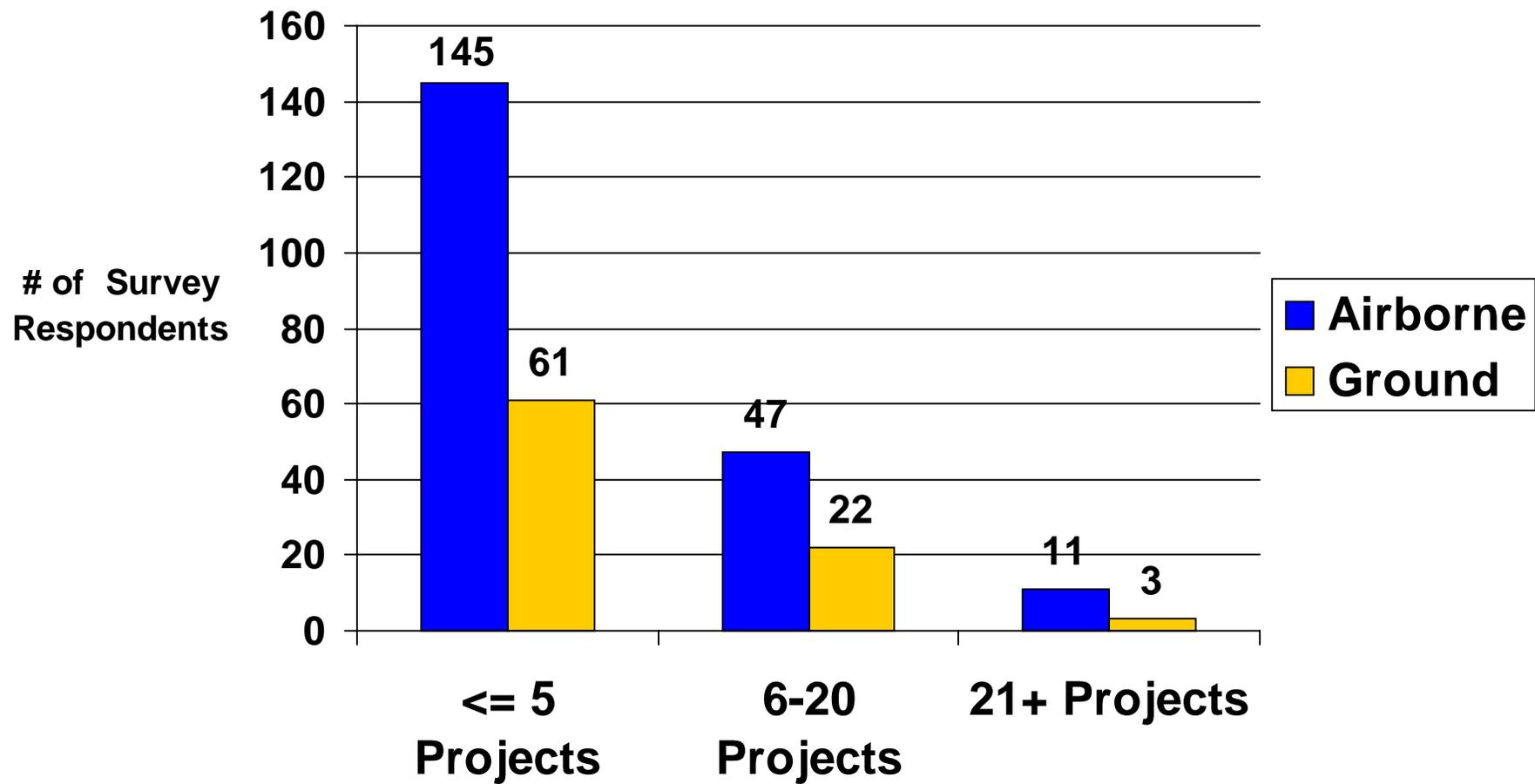


Respondent Profile: Company Type



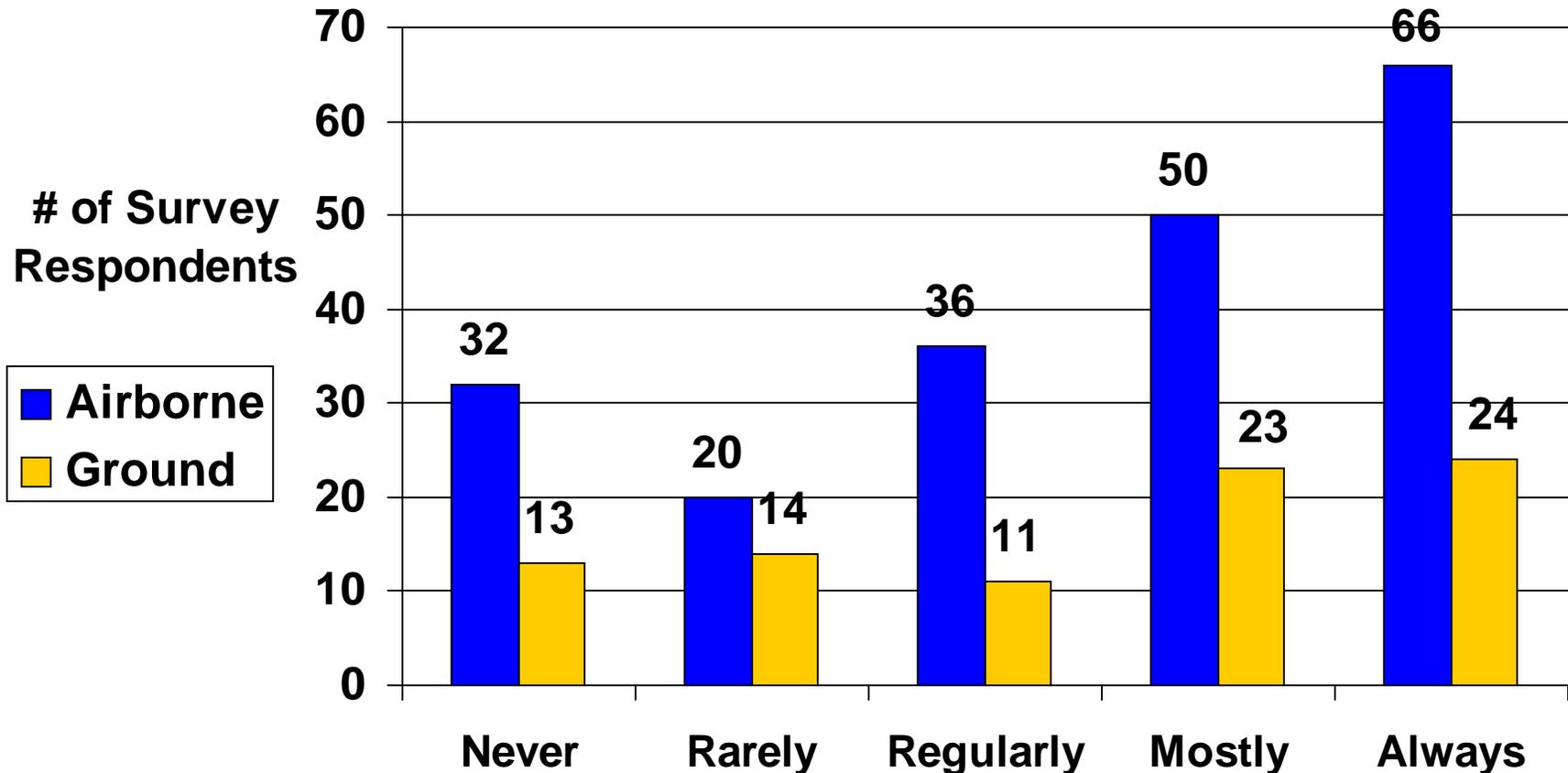


Respondent Profile: Experience with DO-178B



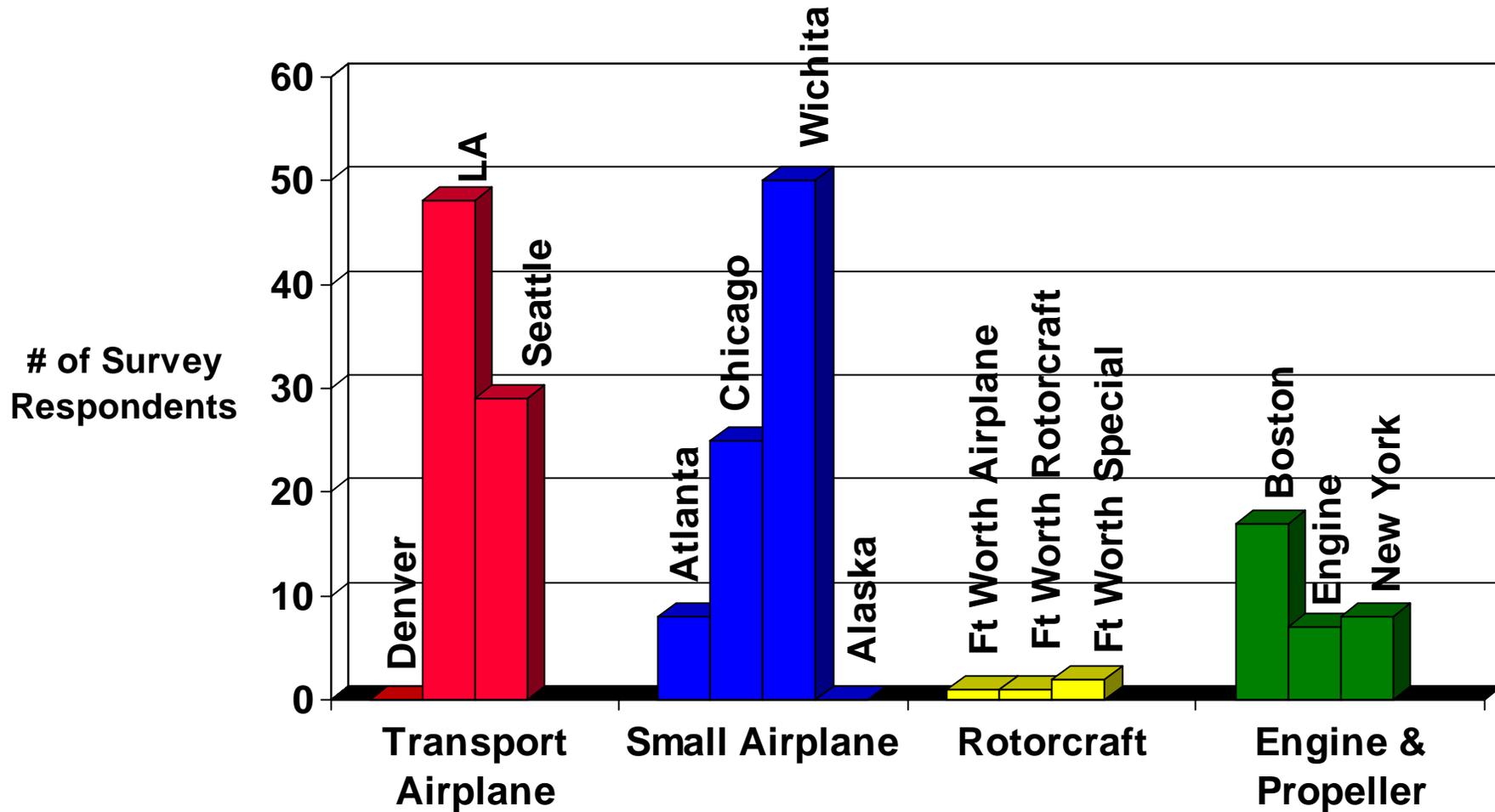


Respondent Profile: Experience with Critical Software (Level A or B)



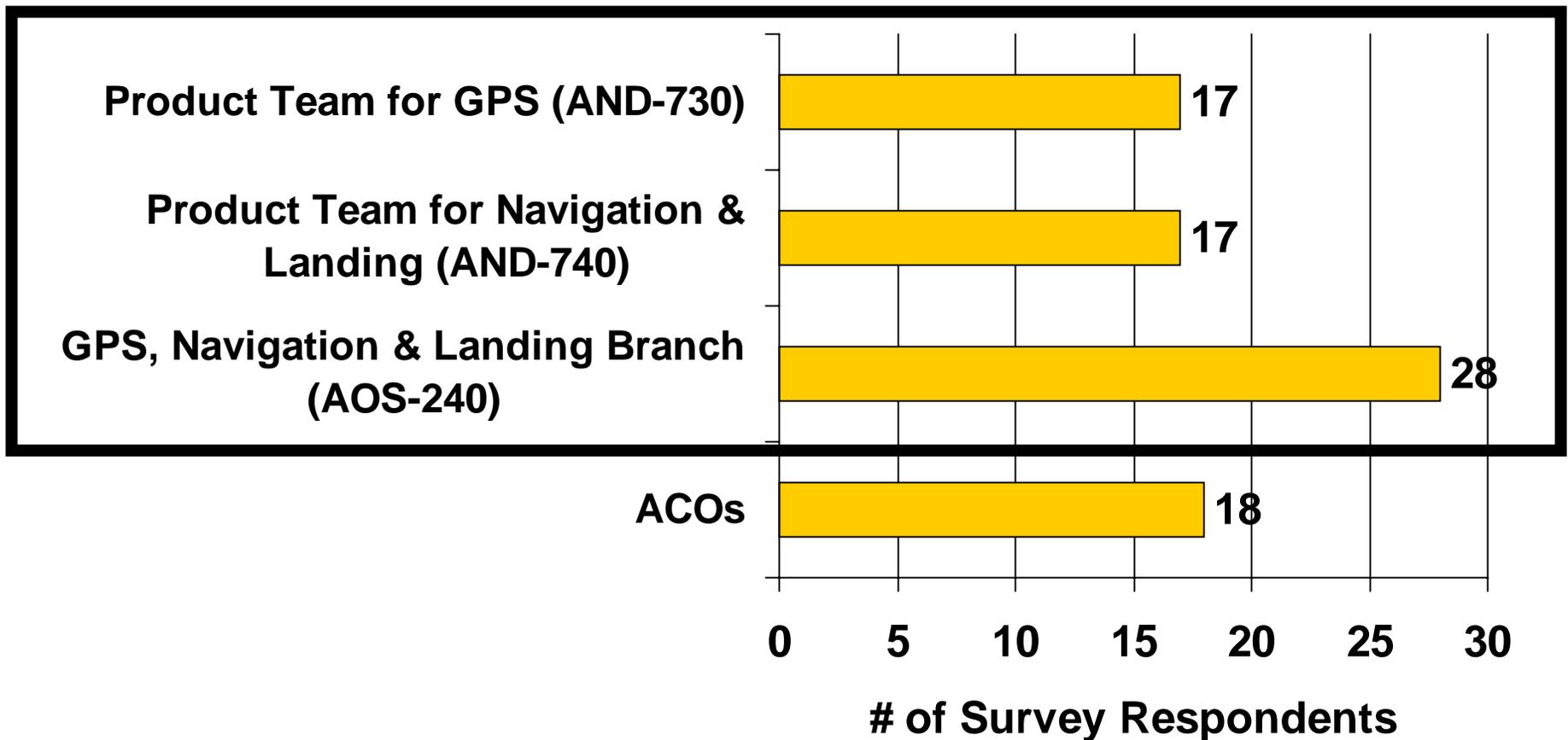


Respondent Profile (airborne): Distribution by ACO





Respondent Profile (ground): Ground-based Approving Authorities





Issues Covered in Survey

Interactions with approving authorities for both airborne and ground-based systems

Software policy & guidance

Effectiveness of specific activities in DO-178B:

- independence
- MCDC
- quality assurance
- traceability
- tool qualification
- documentation

Connection between DO-178B and safety

DER system



Interactions with Approving Authorities

Workshop I Assertion:

**Inconsistencies exist among
ACOs and other approving
authorities in interpreting and
following policy and guidance**



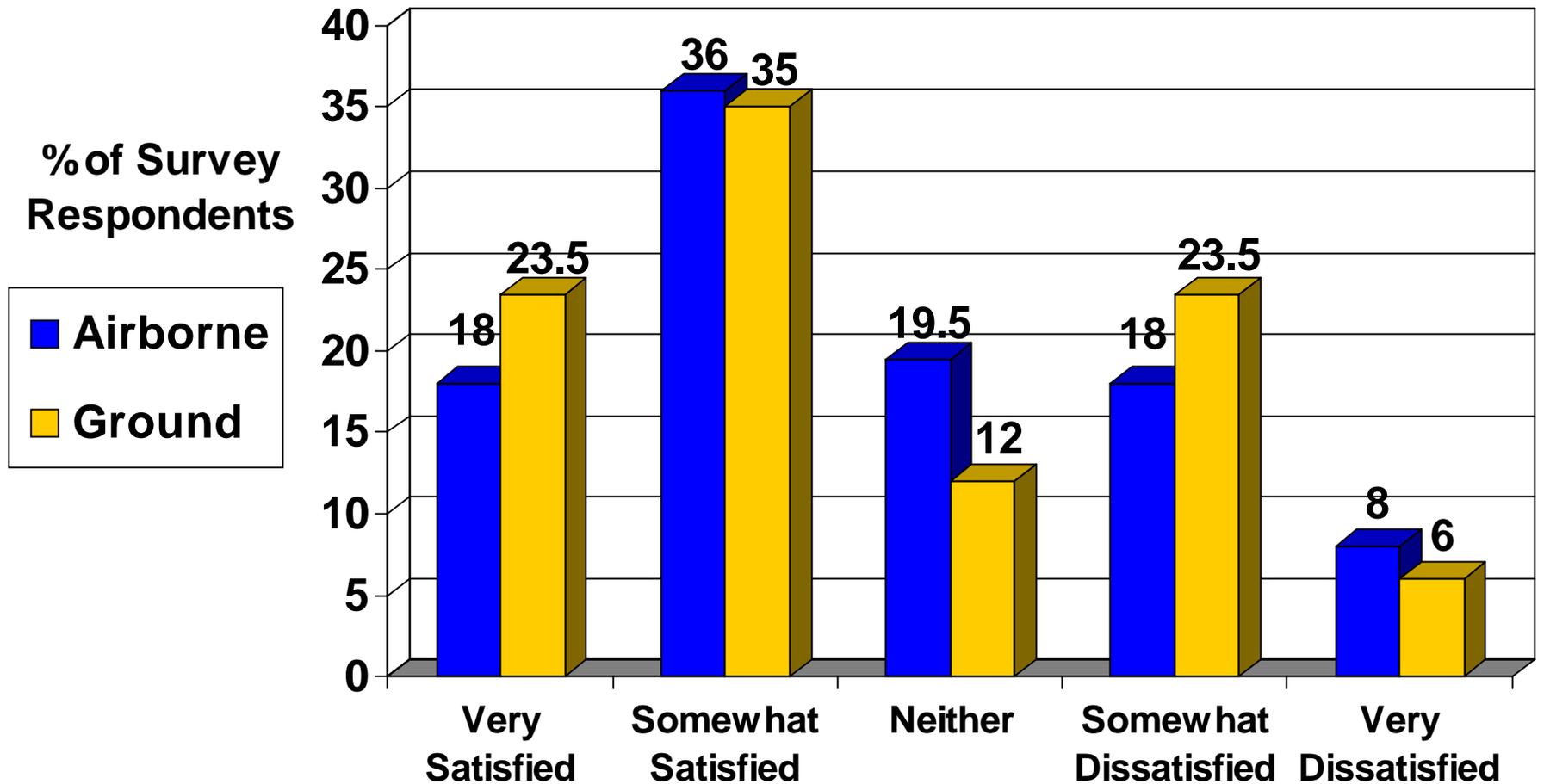


Interactions with Approving Authorities

- What is the general level of satisfaction with approving authorities?
- Communication with approving authorities
 - interacting with applicants
 - addressing certification issues
 - honoring agreements
- Consistency
 - within a single organization; e.g. within an ACO
 - between 2 or more organizations
 - between air and ground



Overall Satisfaction with Approving Authorities





Communication with Approving Authorities

- Problem areas in interacting with applicants (*fair* or *poor* rating)

	Airborne	Ground
Honoring dates for reviews & approvals	31%	29%
Coordinating with technical resources	55%	36%
Responding to submitted plans	53%	50%

- Instances with agreements not being honored

	Airborne	Ground
Verbal agreements not honored	50%	50%
Written agreements not honored	20%	26%



Inconsistencies

Determine if there have been instances of inconsistencies

- Are there more than isolated occurrences?
- Do they impact cost & schedule?

Airborne: All ACOs



Inconsistency between ACOs 76% say yes
> 87% occasionally+
> 61% major cost



Inconsistency within individual ACOs 36% say yes
> 70% occasionally+
> 57% major cost

Ground: AND and AOS



Inconsistency between ground-based approving authorities

**Only 3 have worked with both -- but all 3 report inconsistencies*

#1 Inconsistency: Interpretation of DO-178B



Inconsistencies between Air and Ground

- Objectives:
 - Determine if there is a perception that software aspects of airborne & ground-based systems are really different
 - Determine whether DO-178B fits for ground-based systems
 - ◆ note: only asked ground-based folks

	<i>Yes</i>	<i>No</i>
Are there qualitative differences in the development of ground-based systems, as contrasted to airborne systems, that make DO-178B inappropriate for ground-based systems?	15%	85%
Would an independent authority (as the ACO is to an airborne applicant) be appropriate for ground-based systems?	88%	12%



Recommendations for Communication Issues

- ➡ The FAA should identify the minimum staffing needed to efficiently and effectively communicate and coordinate with applicants.

- ➡ The FAA should examine the circumstances leading to nullification of agreements.

- ➡ The FAA and applicants should document agreements up front. The FAA should develop and implement processes and supporting policy for managing agreements.



Recommendations for Inconsistency Issues

- ➡ The FAA should investigate the root cause(s) of inconsistencies in software guidance, interpretation, and procedural requirements.
- ➡ The FAA should implement a plan to phase in compliance with DO-178B for ground-based systems.
- ➡ The FAA should investigate the feasibility of implementing a regulatory authority independent of the acquisition body for ground-based systems.



Software Policy and Guidance

Workshop I Assertion:

**Insufficient information is available
about the certification process**





Software Policy and Guidance

Written Policy & Guidance: includes FARs, DO-178B, FAA Notices, FAA Orders, Advisory Circulars, and FAA policy memos

- What is the level of satisfaction with software policy & guidance in general?
- Is sufficient information about the certification process available?
- What is the level of satisfaction with specific areas of software policy & guidance?
 - Information on life cycle processes
 - ◆ requirements, design, verification, etc.
 - Information on additional considerations (DO-178B Section 12)
 - ◆ COTS software, partitioning, tool qualification, etc.



Satisfaction with Policy & Guidance

- General satisfaction with software policy & guidance

Somewhat or Very Satisfied

42%

Somewhat or Very Dissatisfied

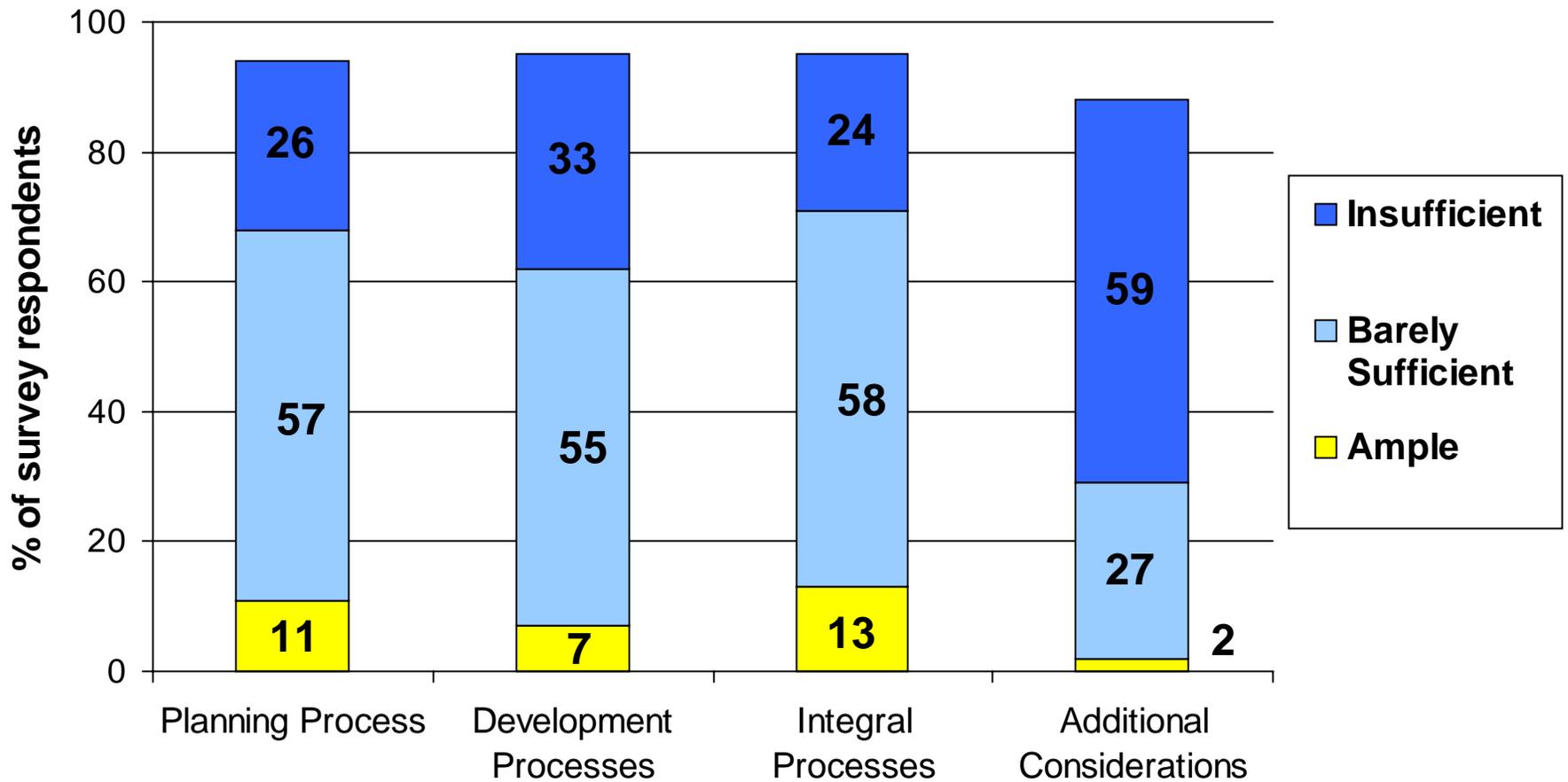
30%

- Not a function of experience with DO-178B, experience with critical software, or software engineering experience

- Availability of Information about the certification process
 - most agree information is available about:
 - ♦ software levels, coordination with approving authorities, audits, TSO, PMA, etc.
 - >52% believe that sufficient information is NOT available for interpreting DO-178B



Satisfaction with Specific Areas of Software Policy & Guidance





Recommendations for Software Policy & Guidance

- ➡ The FAA and the industry, in conjunction with RTCA, should determine the appropriate means for providing information for all life cycle processes. For example, the FAA and industry should determine what is needed to supplement & clarify DO-178B for all life cycle processes.
- ➡ The FAA should take the leadership in the development of policy & guidance for all additional considerations (Section 12 in DO-178B).
- ➡ The FAA should develop a mechanism for providing better information on the intent, interpretation, and application of DO-178B.
- ➡ The FAA should continue efforts to make software-related documentation and training materials available on the web.



Effectiveness of DO-178B Activities

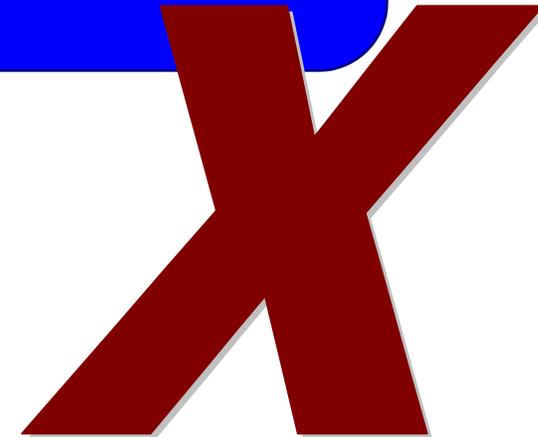
- Independence
- Modified Condition Decision Coverage
- Traceability
- Quality Assurance
- Documentation
- Tool Qualification

- Are each of these activities understood?
- Are each of these activities valuable?
 - Would you do it if not required by DO-178B?
 - Has it provided any benefit?
- How much does it cost & how much time does it take?
 - None, ..., prohibitive amount



Independence

Workshop I Assertion:
Independence adds no value





Independence

- Definition of independence seems to be well understood (86%)
- General satisfaction with independence requirements
 - 63% *somewhat* or *very satisfied*
 - 9% *somewhat* or *very dissatisfied*
- Requirements considered *extremely* or *somewhat valuable* (82%)
- Cost & time burden mixed:
 - 44% *negligible* or *small*
 - 48% *substantial*
- ➡ Recommendations: none
 - that is, independence requirements should not be changed



MCDC

- 60% of respondents have experience with Level A software
 - about 3/4 of those are airborne
 - about 1/4 of those are ground-based
- 79% say MCDC is *moderately* or *extremely difficult*
21% say MCDC is *moderately* or *trivially simple*
- Different Approaches:
 - requirements-based test with additional tests to meet structural coverage (59%)
 - structural testing independent of requirements-based testing (33%)
- 75% say that cost & time for MCDC is *substantial* or *nearly prohibitive*



MCDC

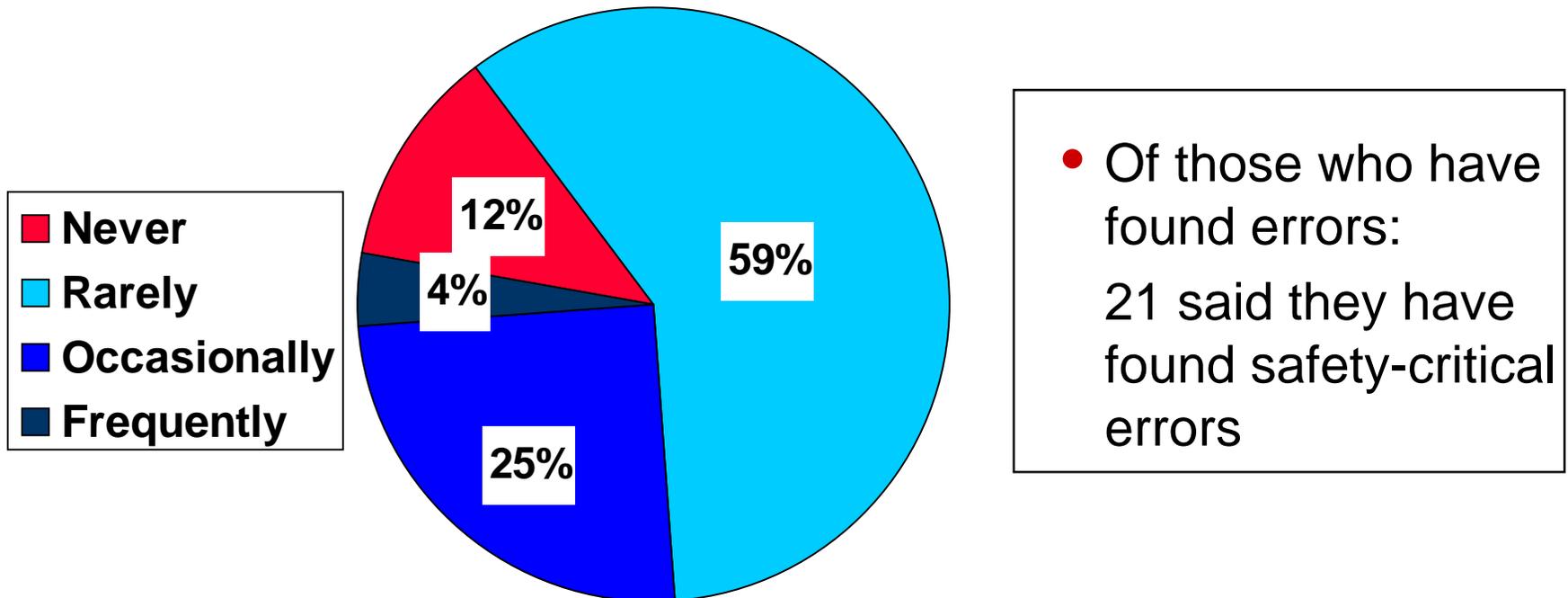
Workshop I Assertion:
MCDC does not find errors

X



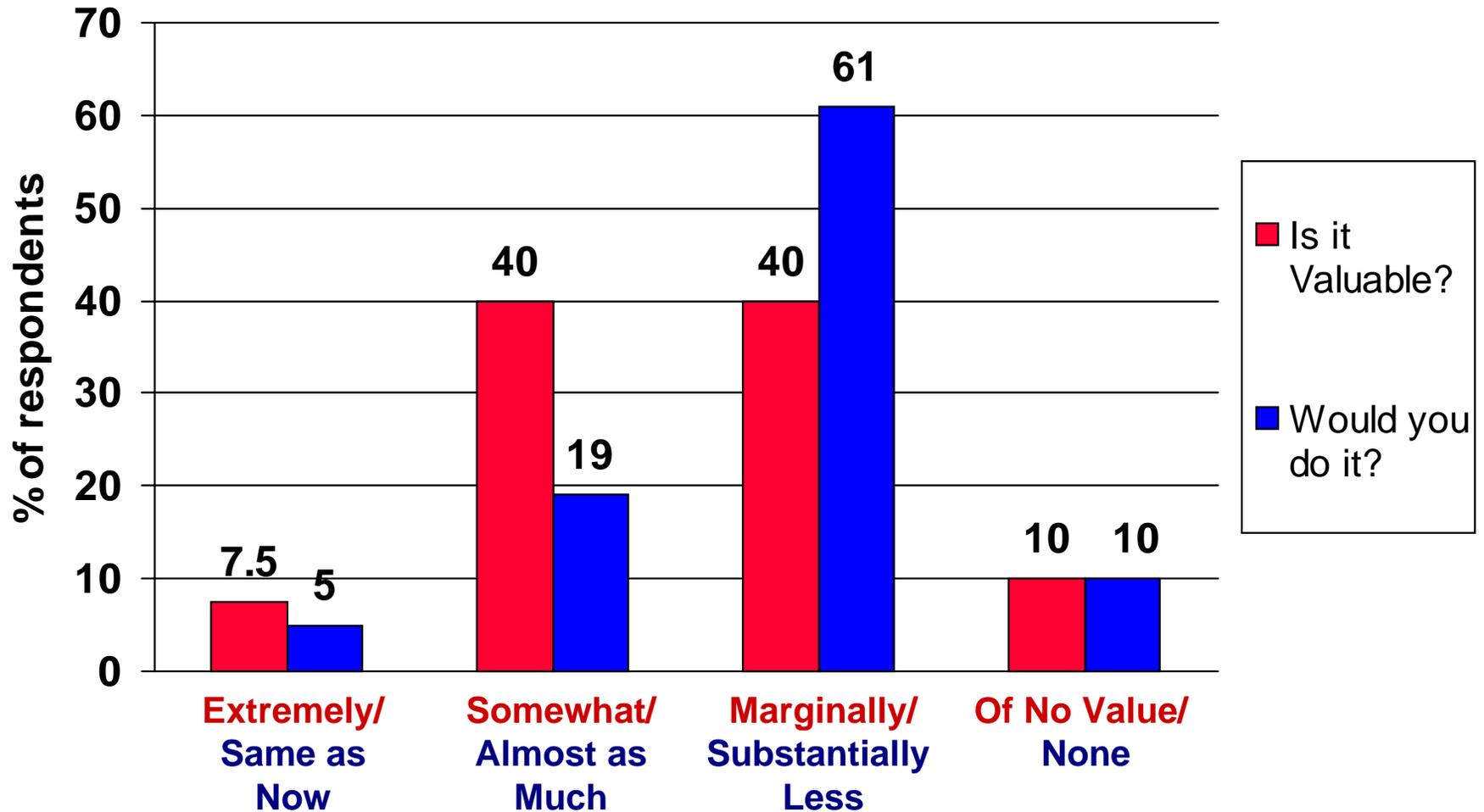
MCDC -- Effectiveness

Frequency with which errors have been found with MCDC





MCDC -- Value





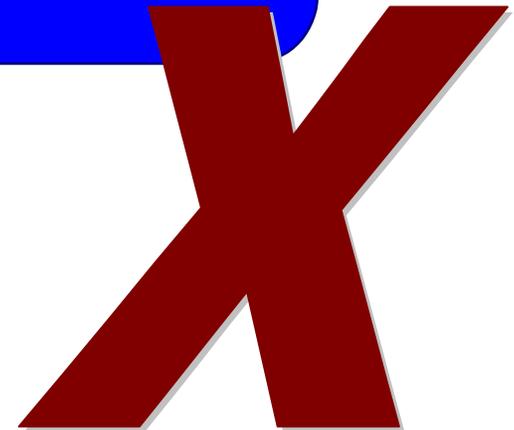
Recommendations for MCDC

- ➡ The FAA and the industry, in conjunction with the RTCA, should document the intent of the MCDC objectives and means for achieving MCDC. In addition, a tutorial should be developed for performing and evaluating MCDC.
- ➡ The FAA should initiate research to explore cost effective means for achieving MCDC or its intent.



Traceability

Workshop I Assertion:
Traceability does not add value





Traceability

- Traceability is generally used effectively
 - for requirements coverage, regression analysis, change impact analysis
 - only 2 respondents used traceability for certification only
- Traceability from source to object code shows misunderstandings
 - 27% document source to object code, regardless of software level
 - 26% of those who do not document traceability from source to object say they *always* work on Level A systems
- Cost & time is *substantial* -- but most would do the *same* or *almost as much as now*



Recommendations for Traceability

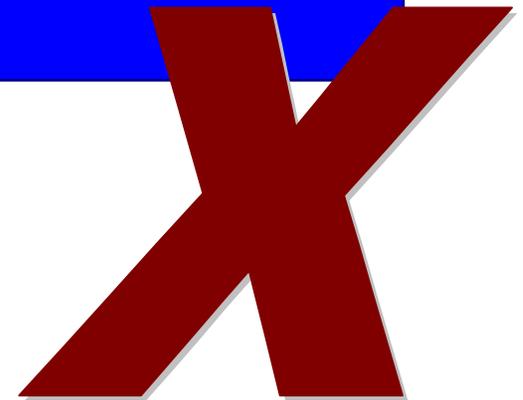
- ➔ The FAA and the industry, in conjunction with the RTCA, should clarify the intent of DO-178B with respect to source to object code correspondence. The FAA should develop policy to standardize the application of source to object code correspondence.



Quality Assurance

Workshop I Assertion:

Quality Assurance does not add value





Quality Assurance

<u>SQA Objective</u>	<u>Somewhat or Extremely Valuable</u>	<u>No Value</u>
1: compliance with plans	79%	3%
2: transition criteria	57%	12%
3: conformity review	72%	5%

- Mixed reaction to cost and time:
 - 58% say cost and time are *small or negligible*
 - 32% say cost and time are *substantial*
 - ➔ companies with a large volume of DO-178B projects report smaller cost than those companies with a limited volume of approvals
- ➔ Recommendations: none



Documentation

Workshop I Assertion:

**FAA makes unreasonable requests
for documentation and packaging**





Documentation

- Packaging & Format:
 - most follow the format given in Section 11
 - ◆ in accordance with company procedures (59%)
 - ◆ by choice of ACO or DER (23%)
 - few have experienced rejection based on format (16%)
 - ◆ ACO requirements and personal preference were cited for the majority of those rejections

- Submittals (certification data submitted to an approving authority)
 - 34% indicated that requests have been made for data/documentation not required by DO-178B or the FARs
 - ◆ however, many examples given were legitimate to ask for
 - clear misunderstandings about certification data



Documentation

Have requests been made 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%

- **61% claim that certification has been delayed as a result**



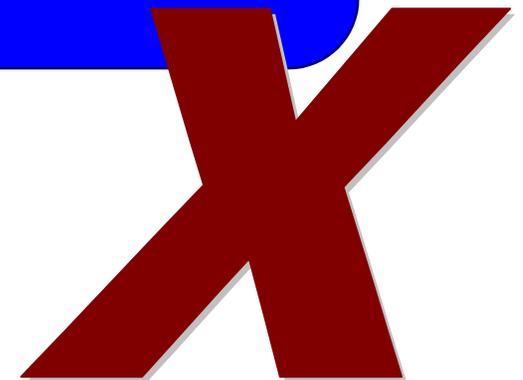
Recommendations for Documentation

- The FAA should make compliance requirements explicit for DO-178B Section 11.
- The FAA should make compliance requirements explicit regarding the data required for certification.
- The FAA should investigate the reason for end-of-project updates to software data or documentation that had no impact on the approval or continued safety or maintenance of the product.



Tool Qualification

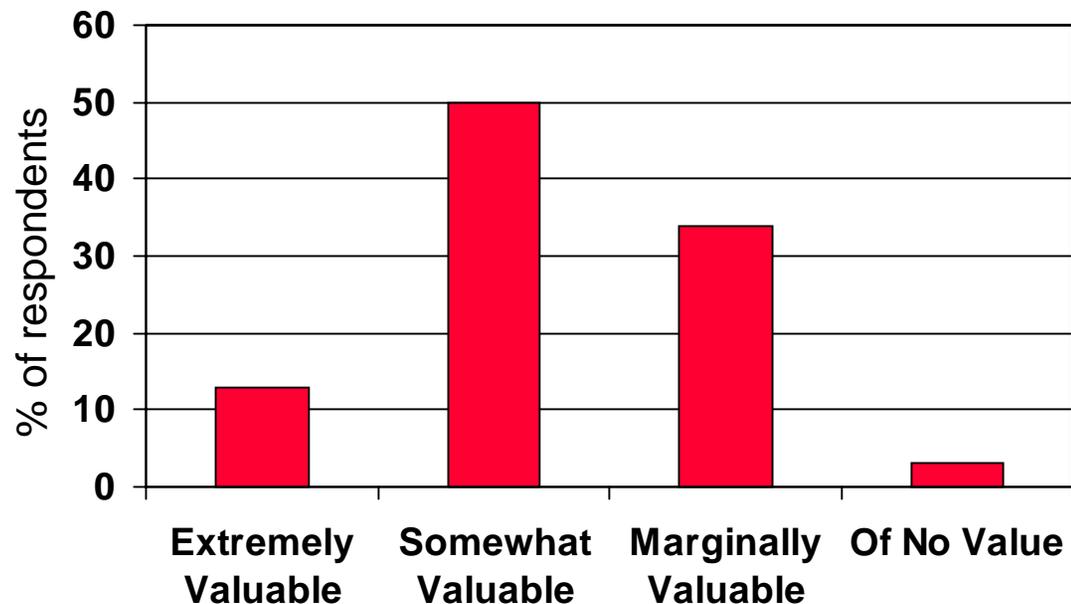
Workshop I Assertion:
Tool Qualification does not find errors





Tool Qualification

- Errors have been found during tool qualification
 - 44% found an error in a development tool
 - 57% found an error in a verification tool
- Cost is perceived to be *negligible* to *small* by 60%, and *substantial* by 36%
- Most perceived the requirements for tool qualification as valuable





Recommendations for Tool Qualification

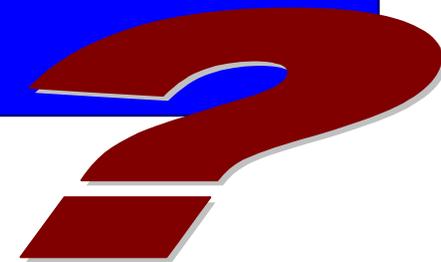
- ⇒ The FAA should clarify compliance requirements and intent for tool qualification. In addition, the FAA should clarify the definitions of development and verification tools.
- ⇒ The FAA and the industry should investigate techniques for tool qualification that will allow qualification to be faster and cheaper. The FAA should determine the feasibility of a national repository for qualified tools and the acceptance criteria for the use of these tools.



Safety

Workshop I Assertion:

DO-178B inadequately addresses the effect of software on the safety of the overall system





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**



Recommendations for Safety

- ⇒ Study should be undertaken on the relationship between DO-178B and safety and the activities actually performed by the industry to ensure system safety.
- ⇒ The FAA should clarify compliance requirements and intent for derived requirements.



DER System (airborne)

Workshop I Assertion:

**The DER system has
inadequacies, inconsistencies,
and inefficiencies**



DER System (airborne)

- Overall, satisfaction is high -- except in the area of 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%

- 53% report that software DERs have approved data on TSO projects



DER System (airborne)

A few problem areas:

- 20% report working with DERs with an inadequate background
 - including lack of software engineering, DO-178B, and certification knowledge
- < 15% report problems in DER/ACO interactions
 - including disputes and rejected proposals of delegation
- 38% report working on projects where software DERs had overlapping responsibilities
 - 41% of those indicated that disagreements led to schedule delays and wasted resources



Recommendations for the DER System (airborne)

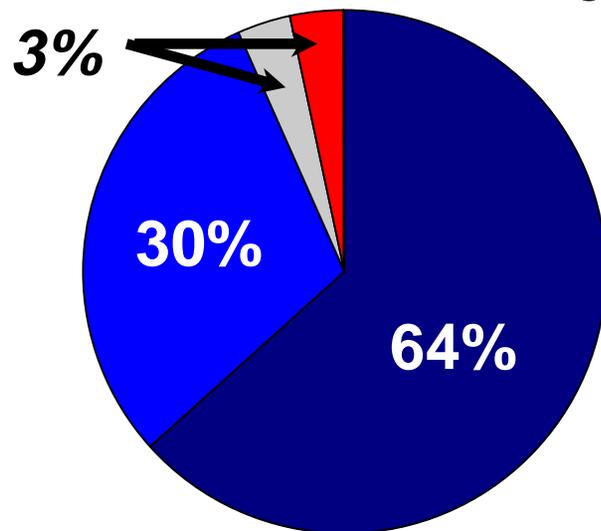
- ➡ The FAA should evaluate the adequacy of their current criteria for selecting software DERs and the procedures to ensure that the DERs meet the competency levels.
- ➡ The FAA should investigate whether software DERs should participate officially in findings of compliance on TSO projects.



Using DERs on Ground-based Systems

No DER-equivalent function in FARs for ground-based systems

Satisfaction Rating



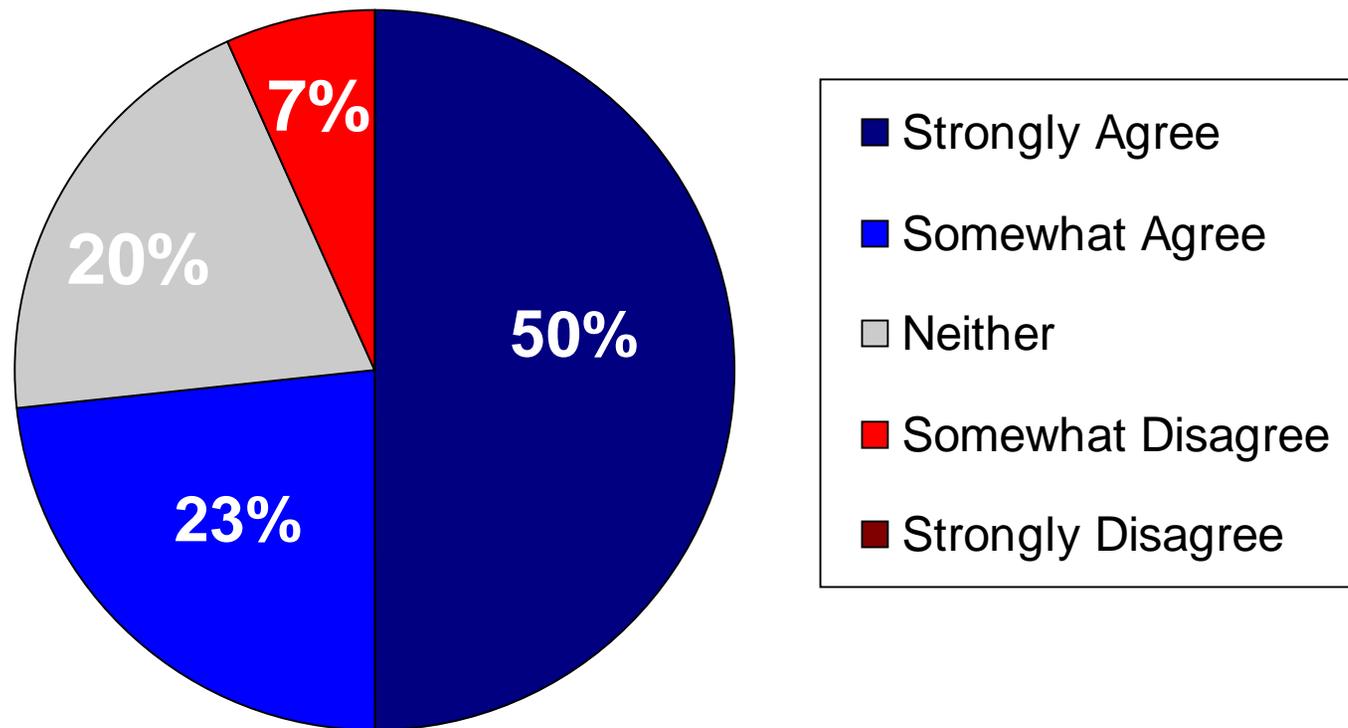
- Very Satisfied
- Somewhat Satisfied
- Neither
- Somewhat Dissatisfied
- Very Dissatisfied

Of the 30 respondents who have worked with a software DER on a ground-based system

- 93% report improved ability to understand & comply with DO-178B
- 82% report reduced delay in approval of submissions



Should the FAA expand the authority of software DERs for a ground-based system?



- ➔ The FAA should investigate expansion of Title 14 CFR Part 183, Representatives of the Administrator, to allow designee authorization for the ground-based community.



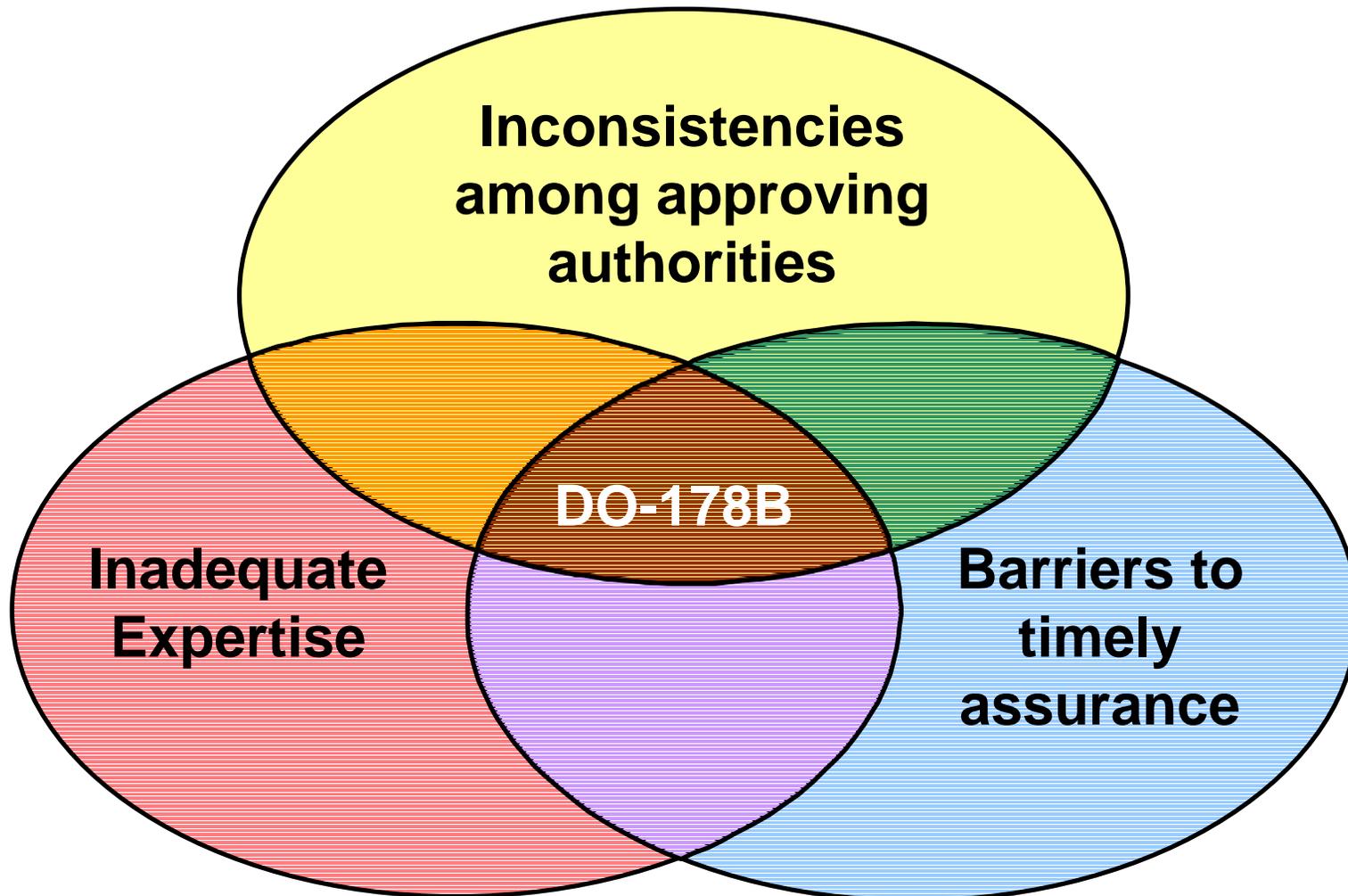
Summary of Issues

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: <ul style="list-style-type: none"> - independence does not add value - MCDC does not add value/find errors - quality assurance does not add value - traceability does not add value - unreasonable requests for documentation - tool qualification does not add value/find errors 	Refuted Refuted Refuted Refuted Validated Refuted
Connection between DO-178B and safety	More data needed
Inadequacies in the DER system	Validated



General Observations

- We have 6 general observations based on the survey findings





Observations about Inconsistency

Aircraft Certification Offices and other approving authorities create unnecessary cost burdens through inconsistent guidance, interpretation, and procedural requirements for software-related issues.

Inconsistencies exist between the airborne and ground-based software approval processes that create inefficiencies resulting in added costs for the industry and potentially for the FAA.



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 varies substantially within the industry.



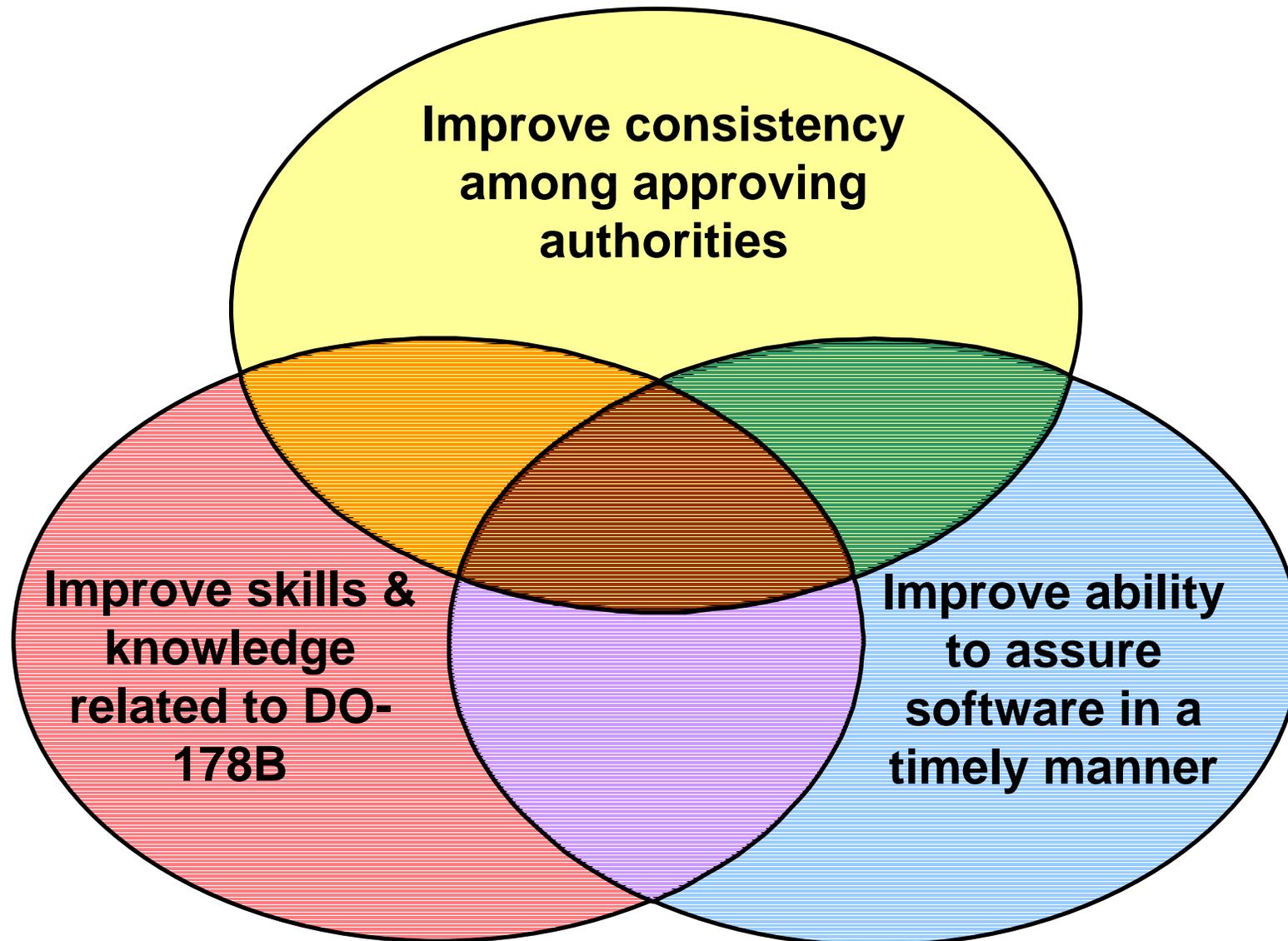
Observations about Barriers

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

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



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 Expertise within the 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 within the agency by:
 - identifying the minimum software staffing needed to assure a consistent approach and timely response for software approvals for all applicants
 - continually assessing software personnel needs and hiring to meet those needs
 - creating, funding, and filling software engineering positions throughout the FAA
 - requiring software engineers who appoint and advise designees for software to meet the same qualifications as the designees



Recommendations to Improve Expertise within the 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.
- 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.