

Challenges in Software Aspects of Aerospace Systems

Kelly Hayhurst
C. Michael Holloway

Presented at the 26th Software Engineering Workshop
Greenbelt, Maryland
November 27-29, 2001



What's Happening?

- FAA modernization programs have overrun cost & schedule because of software problems
 - Standard Terminal Automation Replacement System (STARS)
 - Wide Area Augmentation System (WAAS)
- Software problems contributed to 2 major NASA mission failures
 - Mars Climate Orbiter: English/metric units consistency problem
 - Mars Polar Lander: system requirement failed to make it into the software requirements
- International space station has suffered substantial budget overruns for software



It's Happening Even to the "Best"

Wide Area Augmentation System (WAAS)

Original Cost Estimate (in millions)	Current Cost Estimate (in millions)	Original Scheduled Start Date	Currently Scheduled Start Date
\$892.4	\$2,900.0	1998	2000 2003

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



What's Being Said?

“Information technology is becoming a key part of everything the aerospace and defense industry does for a living, and as the century closes it is computers and software that hold the keys to the future.”

David Hughes, *Aviation Week & Space Technology*

“software development has been the `Achilles Heel` of FAA’s efforts to deliver systems on time and within budget”

- Gerald Dillingham, United States General Accounting Office,
In testimony to Congress about the Wide Area Augmentation System

“Software is ripping apart this industry.”

-Former NASA Administrator Dan Goldin, speaking to the
International Space Symposium



What Are We Doing About It?

- In 1997, FAA asked NASA Langley to lead the *Streamlining Software Aspects of Certification (SSAC)* program
 - to investigate ways 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 program brought the aviation software industry and FAA certification authorities together
 - through workshops to identify fundamental software challenges
 - through an industry-wide survey to collect data to validate those challenges



In the Beginning

215 Complaints

1st Industry Workshop



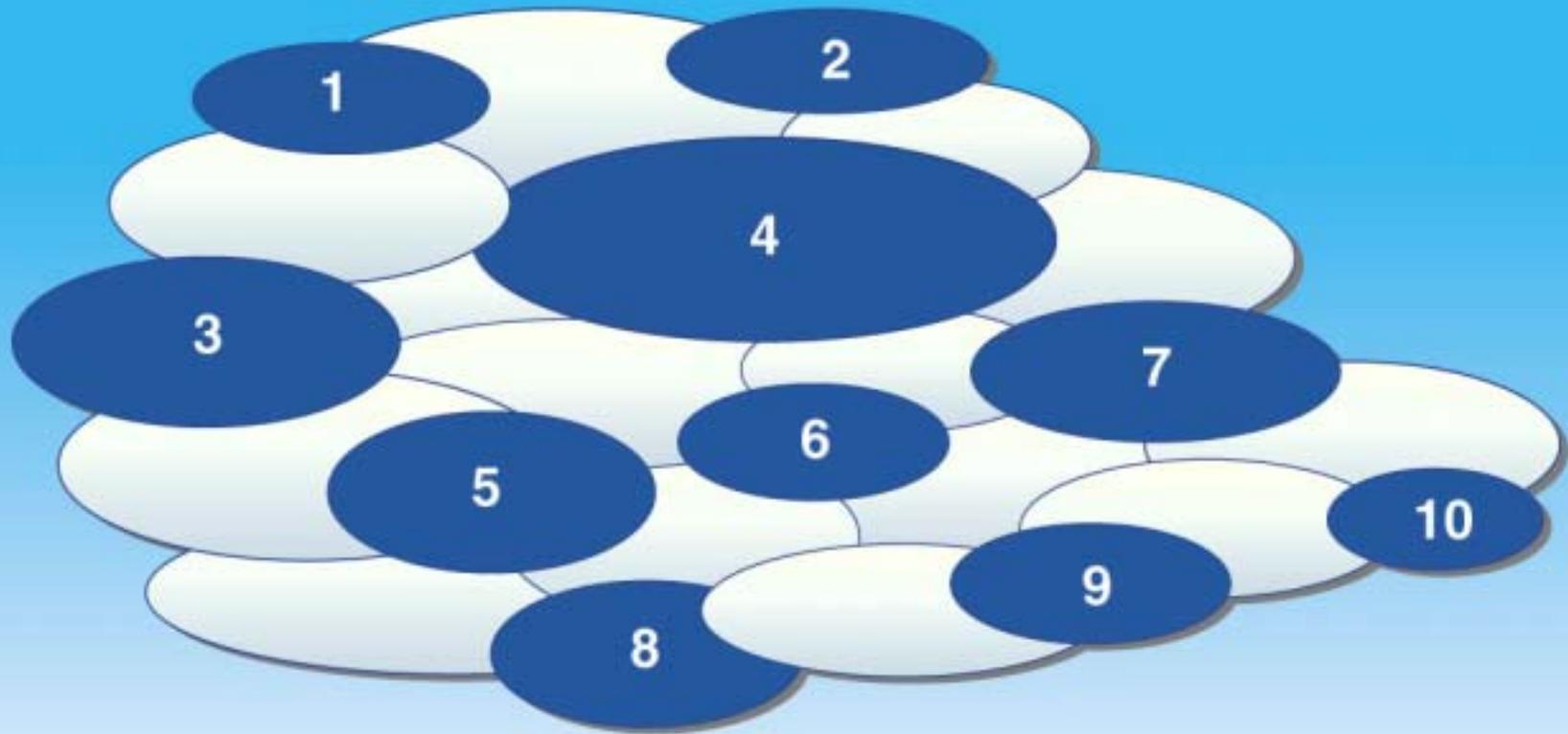
Grouping



Team



Determining Priorities



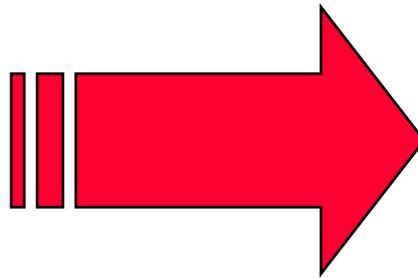
2nd Workshop



Validating

Survey

240 questions to
aviation software
industry



292 completed
surveys
returned
(70+%)

7 of the top 10 issues
validated



Validated Concerns

1. Inadequate information is available about certification
2. Inconsistencies exist within the FAA in interpreting and following policy and guidance
3. Insufficient knowledge of software engineering and related disciplines exists within industry
4. Insufficient knowledge of software engineering and related disciplines exists within the FAA
5. Inadequacies, inconsistencies, and inefficiencies exist in the designee system
6. Lack of cooperation exists between the FAA and industry
7. Requirements definition is difficult



Root Challenges



Example

- Suppose you have the following expression

(A and B) or (B and C) or (A and C)

where A, B, and C are Boolean variables

- To meet verification requirements for Level A software, you need to know the number of *conditions* in this expression

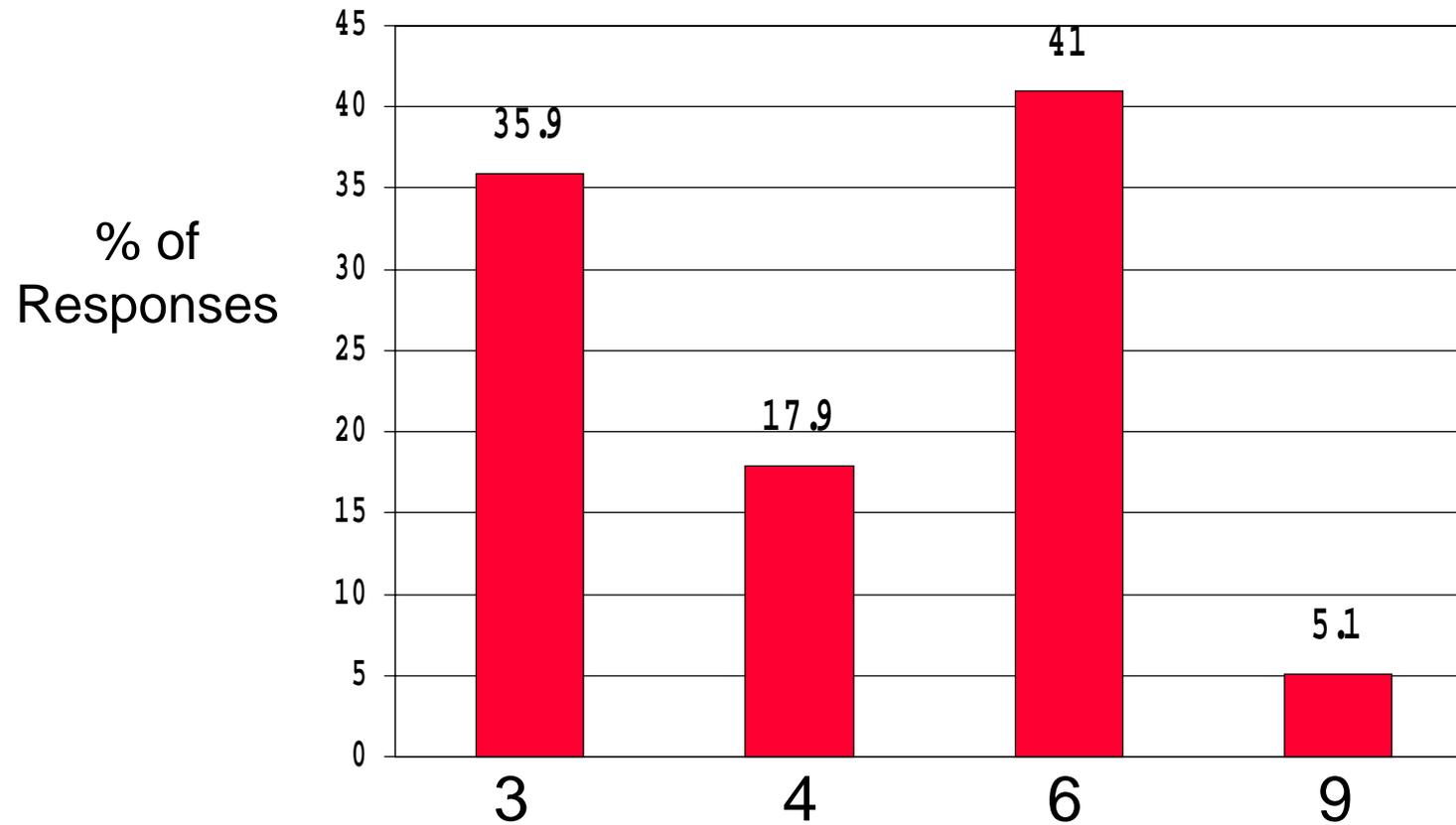
Condition: A Boolean expression containing no Boolean operators (from DO-178B glossary)

How many conditions are there? 3, 4, 6, or 9



The FAA Says...

Distribution of responses from FAA certification authorities



The Answer

6



Explanation

(A and B) or (B and C) or (A and C) has 6 conditions

- The full definition for condition is not contained in the glossary entry for that term
- Part of the definition is given in the entry for decision

Decision: A Boolean expression composed of conditions and zero or more Boolean operators. A decision without a Boolean operator is a condition. **If a condition appears more than once in a decision, each occurrence is a distinct condition.**



Communication Problems

- The glossary entries guarantee differing interpretations
 - definitions distributed across multiple entries
 - terms with strong connotations used in ways that violate those connotations
- Until recently, no clarifying guidance or educational material existed
 - the FAA did not act to develop support material until after the SSAC survey showed the need
 - NASA/TM-2001-210876 *A Practical Tutorial on Modified Condition/Decision Coverage*



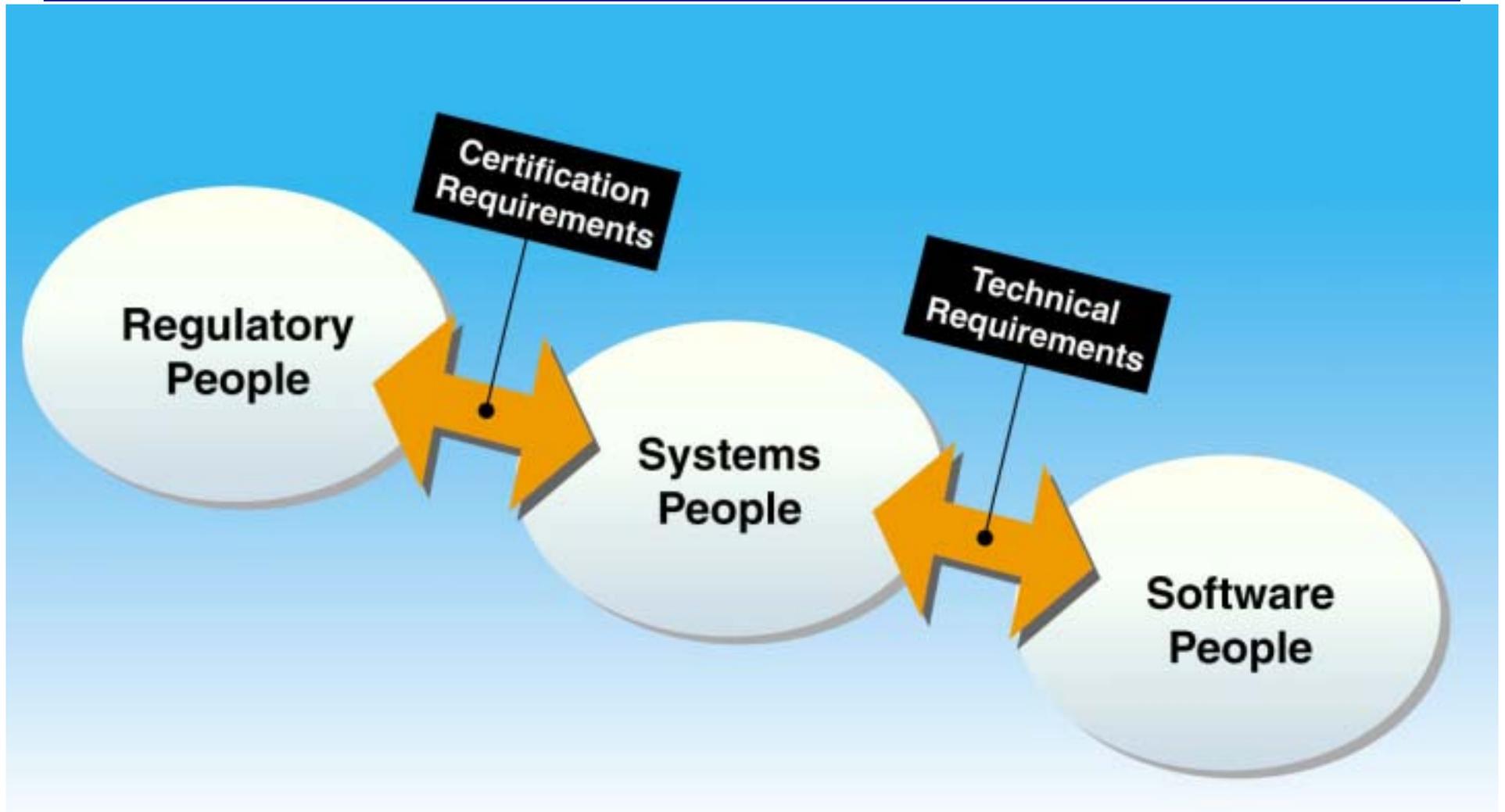
Another Example: Which Is Correct?

Reliability is to **Safety** as

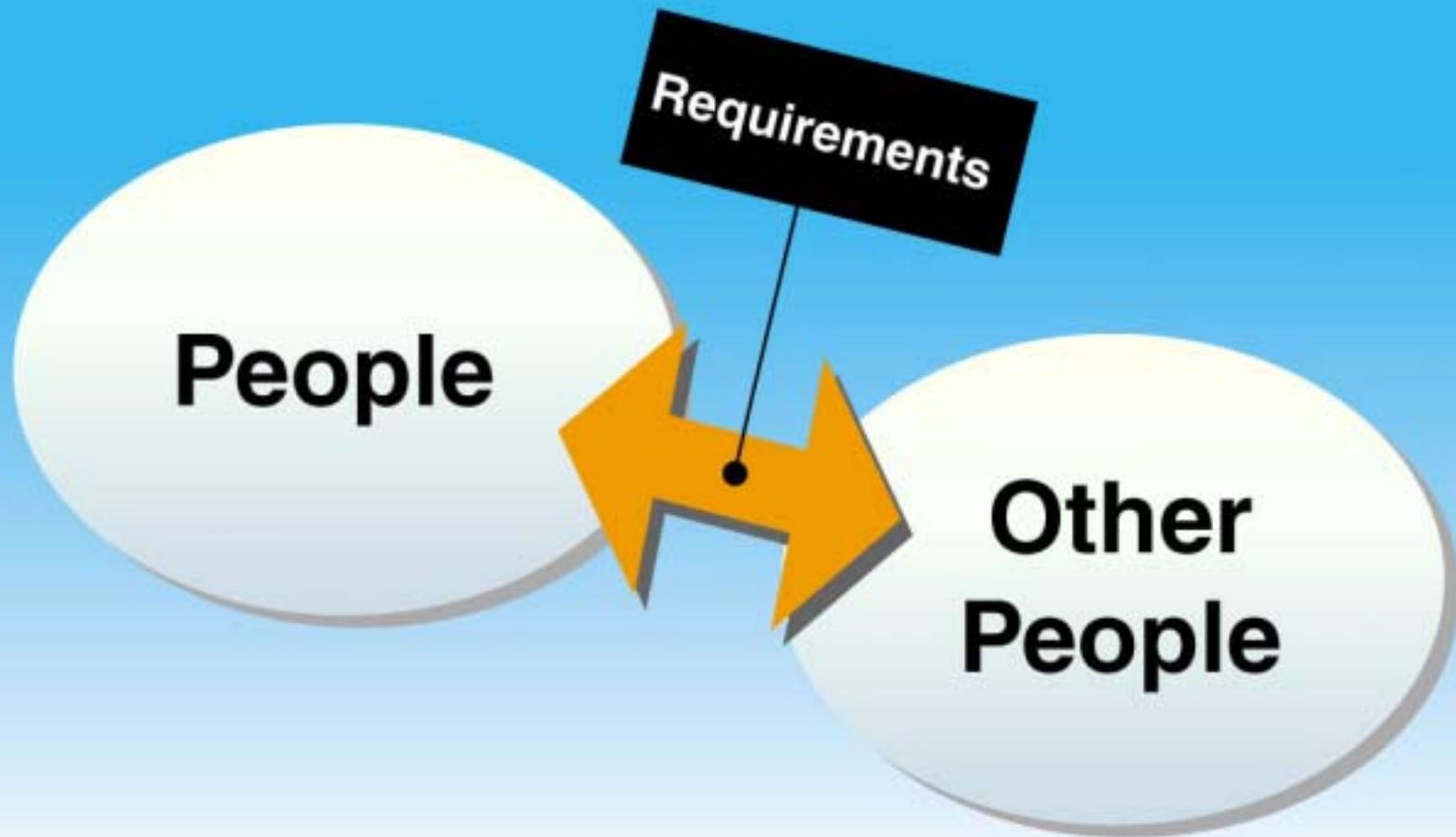
- a. **Water** is to **Life**
- b. **Football** is to **Soccer**
- c. **Legality** is to **Morality**
- d. **Stereo** is to **Speakers**
- e. **Fire** is to **Ice**



Communication Channels Simplified



Further Simplification



The Bottom Line

- **The challenge** in software aspects of aerospace systems is communicating requirements between groups of people
 - Consistently
 - Completely
 - Concisely
 - Promptly
- Improving the communication of requirements is essential for real progress in efficient development of safe and reliable aerospace systems
 - Research efforts should concentrate here
 - Extending “requirements engineering” work to include a broader range of requirements seems promising



Additional Information

- SSAC project
 - <http://shemesh.larc.nasa.gov/ssac/>
- MC/DC tutorial
 - <http://shemesh.larc.nasa.gov/people/kjh/>
- FAA Aircraft Certification Service software information
 - <http://av-info.faa.gov/software/>
- NASA Langley formal methods team work
 - <http://shemesh.larc.nasa.gov/fm/>

