

2003 FAA National Software Conference

SW Service History: Research and Handbook



Software Service History Research Results and Using the Handbook

Ferrell and Associates
Consulting, Inc.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 1



Outline

- Research Effort
- Handbook
- Report
- Research Conclusions
- Application to WAAS
- Conclusions
- Observations
- Future Research



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

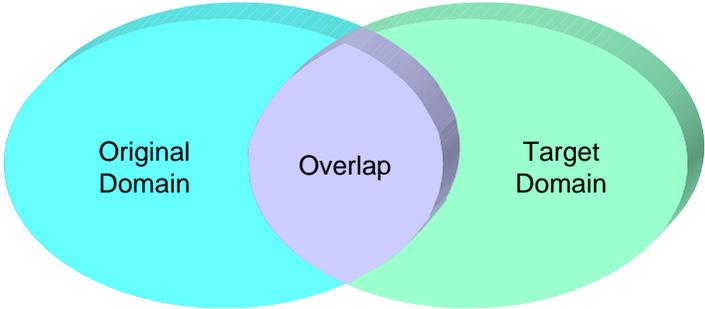
Slide 2

2003 FAA National Software Conference

SW Service History: Research and Handbook



Domain Intersection



“Product Service History – A contiguous period of time during which the software is operated within a known environment, and during which successive failures are recorded.”



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 3



Service History And DO-178B

- Service History is one of the alternate methods
- Acceptability for certification credit is dependent on:
 - Configuration Management of the Software
 - Effectiveness of Problem Reporting
 - Stability and Maturity of Software
 - Relevance of Product Service History Environment
 - Actual Error Rates
 - Impact of Modifications



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 4

2003 FAA National Software Conference

SW Service History: Research and Handbook



Software Service History Research

Although Service History seems to be a fairly straightforward technique, in practice, such use has proved extremely problematic because of the following:

- Difficulty in proving relevance of environment
- Consistency in the measure of historic performance (scattered data because of many "user" airlines)
 - Effectiveness of problem reporting
 - Stability/Maturity of software
 - What is the minimum "duration" of data at different criticality levels
 - How to compute "error rates"

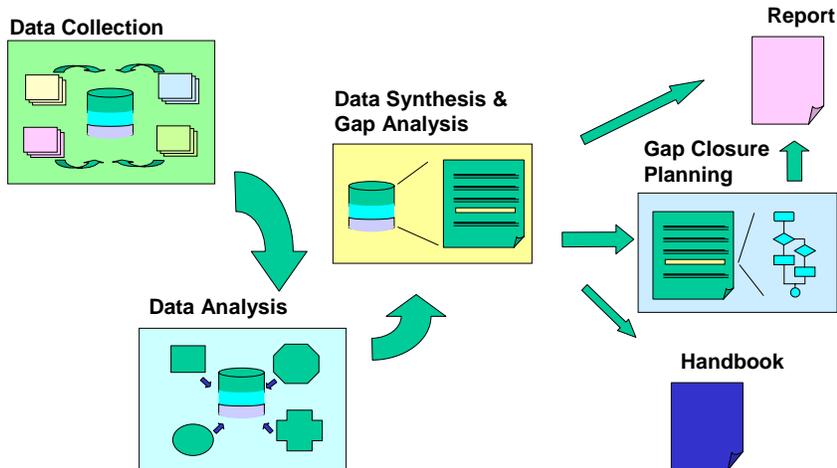


Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 5



Overall Process



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 6

2003 FAA National Software Conference

SW Service History: Research and Handbook



Handbook Outline

- Introduction
- DO-178 Framework
 - The definition
 - **Analysis of Product Service History in DO-178B**
 - Relationship with Previously Developed Software
 - Product Service History Vs. Software Reliability
- The Elements of Product Service History
 - Questions of Problem Reporting
 - Questions of Operation
 - Questions of Environment
 - Questions of Time
- Adequacy of the Development Process
- Establishment of “Equivalent Safety”
- Summary
- Bibliography
- **Appendix A: Evaluation Worksheets**

DOT/FAA/AR-01/116

Software Service History Handbook



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 7



Analysis of PSH Guidance in DO-178B

- Table 1 of the Handbook provides a detailed review and analysis of the eleven guidance statements for the use of product service history found in DO-178B, section 12.3.5
- This table is designed to help you understand the underlying rationale behind each of the guidance statements by providing:
 - A set of observations on what is being discussed and where some of the pitfalls may be in satisfying that guidance statement
 - An initial round of questions to ask regarding the available data
 - A clear linkage back to the elements of the definition of PSH through the Questions metaphor used throughout the Handbook
- Use Table 1 to understand “WHY” each guidance statement exists



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 8

2003 FAA National Software Conference

SW Service History: Research and Handbook



Worksheets Overview

- Appendix A contains four worksheets, one for each area of questions relevant to evaluating PSH data.
- The majority of worksheet items relate directly to a section 12.3.5 item.
- A small number of items that represent best practices from other industry sectors have also been included.
- The intent is that these worksheets would be used in the preparation of an alternates means of compliance argument.
- There is NO requirement from the FAA that you must use these – they are simply an aid to you!
- The worksheets should not be considered static – you may need to tailor them for a particular project.



Research conducted for the FAA under contract#: DTFA0300P10138
 Ferrell and Associates Consulting, Inc.

Slide 9



Sample Worksheet

Table A-1. Worksheet for Questions of Problem Reporting

Area:	Problem Reporting/ Configuration Management	Software Being Evaluated:	
Project:		Evaluator:	
Date:			

	DO-178B Reference	Question	Response	Issues
1.	12.3.5 a and c	Are the software versions tracked during the service history duration?		
2.	12.3.5 a and c	Are problem reports tracked with respect to particular versions of software?		
3.	12.3.5 a	Are problem reports associated with the solutions/patches and an analysis of change impact?		
4.	12.3.5 a	Is revision/change history maintained for different versions of the software?		
5.	12.3.5 a	Have change impact analyses been performed for changes?		
6.	12.3.5 b	Were in-service problems reported?		
7.	12.3.5 b	Were all reported problems recorded?		
8.	12.3.5 b	Were these problem reports stored in a repository from which they can be retrieved?		
9.	12.3.5 b	Were in-service problems thoroughly analyzed, and/or those analyses included or appropriately referenced in the problem reports?		
10.		Are problems within problem report repository		



Research conducted for the FAA under contract#: DTFA0300P10138
 Ferrell and Associates Consulting, Inc.

Slide 10

2003 FAA National Software Conference

SW Service History: Research and Handbook



Report Outline

- Introduction
- DO-178 Framework
 - The definition
 - Analysis of Product Service History in DO-178B
 - Relationship with Previously Developed Software
 - Product Service History Vs. Software Reliability
- The Elements of Product Service History
 - Questions of Problem Reporting
 - Questions of Operation
 - Questions of Environment
 - Questions of Time
- Adequacy of the Development Process
- Establishment of “Equivalent Safety”
- Research Summary
- Conclusion
- Appendix A: Data Collection and Synthesis
- Appendix B: Literature Search

DOT/FAA/AR-01/125

**Software Service
History Report**



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 11



Research Conclusions

- Worksheets- lists of general considerations for evaluating service history.
- Worksheets must be customized for each program.
- A list of assurance deficiencies may be derived using these worksheets for a particular program.
- Other available data as well as focused **supplemental** verification may be applied to complete DO-178B objectives.
- Other alternate methods of compliance such as reengineering may also be applied to supplement objective evidence.
- FAA expects all of the objectives to be fulfilled regardless of what mix of methods are used to show compliance.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 12

2003 FAA National Software Conference

SW Service History: Research and Handbook



The WAAS Service History Effort

- Data Collection Catalogue
- Data Source Evaluation
- Problem Reporting Evaluation through Worksheets
- Deficiency Compensated through Other Sources
- Error Rates Using 60-Day Testing
- Data Synthesis and Final Report



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 13



WAAS and Service History Credit

- Research task was to examine available problem reporting data for level D components to address possible use of service history instead of continued development assurance for the maintenance of these components
- Acceptability for certification credit is dependent on:
 - Configuration Management of the Software
 - Effectiveness of Problem Reporting
 - Stability and Maturity of Software
 - **Relevance of Product Service History Environment**
 - Actual Error Rates
 - Impact of Modifications

Highly relevant for WAAS since the environment is not changing



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 14

2003 FAA National Software Conference

SW Service History: Research and Handbook



Data Collection Catalogue

FAA Consulting (FAAC) built a catalogue of all available data sources that may be useful in formulating a service history argument for level D portions of WAAS.

- Developed a format for collecting the data to ensure necessary attributes are captured including:
 - Source
 - Frequency of Update
 - Problem Reporting
 - Configuration Control of Problem Reports
 - Developmental Data
 - Test Data
- It was realized during data collection that in order to extend a possible service history argument, development, transition as well as post-transition plans for WAAS must be examined for appropriateness.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 15



Data Source Evaluation

- Data sources were examined for transition and post transition phases to assure that the environment was appropriate for the collection of problem reports and application of service history.
- Each of the data sources identified in the data catalogue were examined using the evaluation criteria outlined in the Service History Handbook and Report.
- This evaluation started with tailoring of the worksheets contained in Appendix A of the Service History Handbook.
- A core set of data items were identified from which to build the service history argument.
- It was not possible to separate level D specific problem data from WAAS problem report database since problems were reported and resolved at a larger component level.
- Procedures for the maintenance of WAAS were under development during this task.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 16

2003 FAA National Software Conference

SW Service History: Research and Handbook



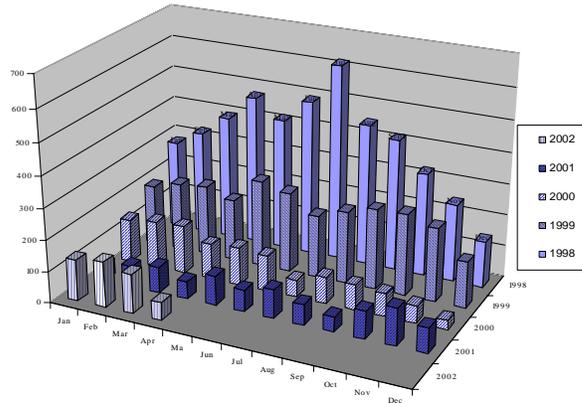
Robust Problem Reporting During Development

Collected during the development of WAAS

Large number of problem reports

Month by month history shows a relatively consistent reduction in the number of problems

Some spikes – associated with major modifications or additions of functionality



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 17

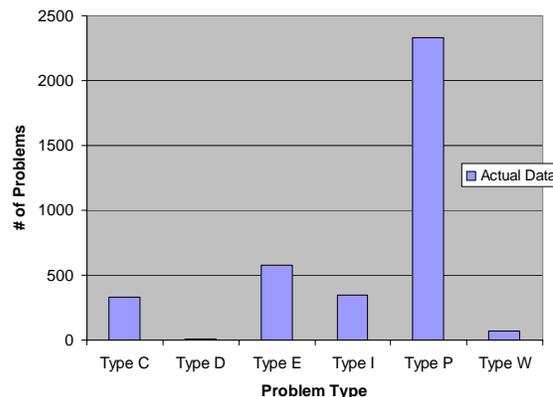


Problem Categorization

Categorization of ALL of the problems in the database

- C = Requirements Change
- D= Documentation Problem
- E= Enhancement
- I and W = "Others"
- P=Software Problems

Is it OK to combine 4 years of data on system under development?



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 18

2003 FAA National Software Conference

SW Service History: Research and Handbook



Problem Reporting Evaluation through Worksheets

- Next task was to examine existing problem reporting mechanisms employed on WAAS by both the prime contractor for WAAS and the FAA during developmental, transition and post transition phases of WAAS.
- This evaluation included:
 - Data Particulars
 - How is it collected (completeness)
 - What “problems” are rejected (e.g., duplication, no fault found)?
 - What problems are consolidated?
 - Configuration control of problem reports
 - Problem resolution and the tie to system changes
 - Safety problem identification



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 19



Application of Worksheets

- Problem Reporting
 - Lack of sufficient granularity in problem reporting
 - Single entry for multiple problems
 - System not stable
 - Safety problems tracked but in a different data base
- Operation
 - COTS problems are not noted in this database
 - COTS upgrades are not tracked along side of problems; their effect on problem reports cannot be tracked
- Time
 - Definition of appropriate service period for WAAS level C needs to be negotiated with certification authorities



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 20

2003 FAA National Software Conference

SW Service History: Research and Handbook



More on Use of Worksheets

- The next task was to identify any gaps in the then current and planned data collection for the WAAS program, as well as any potential problems with the data that was collected that could invalidate a service history argument or prevent its creation.

Process checks on problem reporting, quality of data, problem collecting, configuration control of problems, connection to safety and hazard tracking, and associated software version tracking.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 21



Deficiencies Compensated

- FAAC conducted a trade study of potential approaches to mitigate the data gaps and recommended approaches most likely to provide a robust service history approach for WAAS. Can missing data be recreated using existing data?
 - Validity of existing data given the system's state of flux
 - Effects of missing data on completeness and cogency of overall service history argument
- Since the developmental data was invalidated because of system instability, focus turned to future processes for WAAS.
 - Are there cost/effort savings by shifting to Service History argument for level D components only?
 - Are there changes in the data collection process that can be made to close the gap in the future?
 - What processes should be in place for the maintenance of WAAS to assure that compliance to Service History argument is not invalidated for the future?



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 22

2003 FAA National Software Conference

SW Service History: Research and Handbook



60-Day Testing

- Although not a part of the original plan, an examination of 60-day testing was added to the research effort as a separate task.
- All of the data collected during the development of WAAS indicated a system under flux and hence could not be used to estimate an error rate for proposal to the authorities for use if service history was to be adapted.
- 60-day stability testing offered a unique opportunity for a systematic conduct of tests and collection of problem data with a frozen system. Further, there were no safety problems observed during this period.
- The results of 60-day testing indicated two errors in level D components per 720 hours of contiguous operation. This figure could be used as a proposed error rate for applying service history if this method of compliance is chosen for level D software.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 23



Synthesis and Report

- FAAC prepared a report detailing all analyses and recommendations derived from the study for an overall candidate service history approach for WAAS.
 - Characterization effect of safety problems on problem reporting
 - Error rate proposal and its relation to system safety
 - Impact of hardware and software modifications on problem report data
 - Impact of maintenance of level D by using service history rather than development data
 - Adequate continued documentation for proper maintenance of software
 - Difficulties with organizational infrastructure and processes



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 24

2003 FAA National Software Conference

SW Service History: Research and Handbook



Recommendation

- Use of Service History for WAAS Level D components will not alleviate the need for continued documentation and development processes since the maintenance of WAAS will be made more difficult if such processes are not in place.
- Although 60-day testing data indicates a failure rate of 1.4×10^{-3} it should be noted that this failure rate cannot be used in the system safety calculations since DO-178B explicitly prohibits the use of software failure rate data in safety calculations.
- Proposed processes for maintenance of WAAS should consider robust problem reporting in order to keep the service history option open for the future in case the system becomes so stable that no frequent or major maintenance is needed for level D software.



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 25



Questions / Observations

- If SW with known problems is fielded using service history, what is the guidance for counting these known errors for subsequent calculations of error rates for future uses of service history upon modification of that SW (which may be in use for decades)?
- How early is too early for the application of service history –even if no safety problems are noted? Although WAAS is accepted by the FAA, many development activities are still underway.
- Guidance is needed for continued computation of error rates when there is a change in the problem reporting process, configuration control and users-Transition of WAAS.
- If the same software (whose service history is being tracked) is being used in more than one system (WAAS and MSAS), should all problem reports be considered for error rates?



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 26

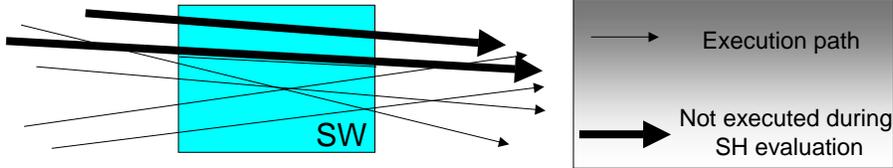
2003 FAA National Software Conference

SW Service History: Research and Handbook



More Questions

- Service History may be viewed as beta testing – verification in the field;
 - How can we assure structural coverage using problem reports?
 - Why does 178B judge the maturity of software by the duration rather than coverage?
 - Would it be possible to combine service history for “normal execution” with focused testing for “abnormal execution?”
 - How does one truly know to what extent the software was executed during the service history period – both a coverage and an environment issue?



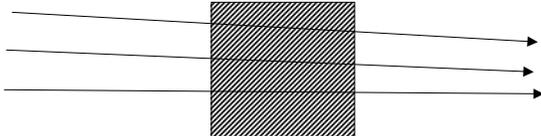
Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 27



More Observations

- DO-178B and SW maintenance: If service history is used as an alternate method for SW that is undergoing repeated modifications, what are the types of design, development, and maintenance documentation needed for safe continued maintenance?
 - Would it be better to limit service history only to portions of software whose “inner workings” are not known and hence there is no possible maintenance on that software?



Black box SW not expected to be updated

Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 28

2003 FAA National Software Conference

SW Service History: Research and Handbook



More Observations

- Should 178C give guidance for maintenance of software that has been assured through “alternate methods”?

Maintenance of SW through alternate methods	Maintenance of SW through developmental process and product verification
Requirements? Design? Code? Change code without design?	Requirements, design, code, verification



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 29



Further Research

- Guidance for the minimum acceptable length of service history duration for different levels given a high quality of problem reporting process and tight configuration control of problem reports-note in DO-278. Shadow systems run the software in exactly the same environment with live data for considerable length of time. Can the same technique be used for airborne software to gain confidence in use of COTS?
- Guidance on tool qualification through service history
 - Differences between the view of “same or similar” environment consideration necessary for proper reuse and the view of broad usage necessary for assurance of a more complete structural coverage of execution of software
 - COTS tool vendors as keepers of problem report history
 - Sharing of tool problems between various avionics manufacturers similar to nuclear domain
 - COTS tool version control



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 30

2003 FAA National Software Conference

SW Service History: Research and Handbook



Contact Information

- If you have questions concerning the content of this presentation or DO-178B issues in general, please contact us at:
Tom (T) or Uma (U) Ferrell
Voice: (703) 757 – 9777
Fax: (703) 757 – 9177
Mobile: (703) 989 – 9777(T) / 9888(U)
Email: tom@faaconsulting.com
uma@faaconsulting.com
Web: www.faaconsulting.com



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 31



Questions and Answers



Research conducted for the FAA under contract#: DTFA0300P10138
Ferrell and Associates Consulting, Inc.

Slide 32