

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

What about A-7.8 ?

Test coverage of software structure (data coupling and control coupling) is achieved.

What was the intention of SC-167 and how can we use their guidance?

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

1

Examine DO-178B “Coupling” and “Flow”

- Partitioning - 2.3.1
 - » ... technique for providing isolation between functionally independent software components to contain and/or isolate faults and potentially reduce the effort of the software verification process
 - » ... should consider ...
 - control coupling: vulnerability to external access
 - data coupling: shared or overlaying data, including stacks and processor registers
- Software Design Process Activities – 5.2.2
 - » The software design process is complete when its objectives and the objectives of the integral processes associated with it are satisfied. Guidance for this process includes:
 - f. Control flow and data flow should be monitored when safety-related requirements dictate, for example, watchdog timers, reasonableness-checks and cross-channel comparisons.
- Reviews and Analyses of the Software Architecture – 6.3.3
 - » The objective of these reviews and analyses is to detect and report errors that may have been introduced during the development of the software architecture. These reviews and analyses confirm that the software architecture satisfies these objectives:
 - b. Consistency: The objective is to ensure that a correct relationship exists between the components of the software architecture. This relationship exists via data flow and control flow.
- Reviews and analyses of source code - 6.3.4
 - » ... ensure that the Software Code Standards were followed ... especially complexity restrictions ... including
 - the degree of coupling between software components, the nesting levels for control structures ...

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

2

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

More DO-178B "Coupling" and "Flow"

- Structural Coverage Analysis - 6.4.4.2
 - » analysis should confirm the data coupling and control coupling between the code components.
- Software Requirements Standards – 11.6
 - » ... Software Requirements Standards ... should include:
 - b. Notations to be used to express requirements, such as data flow diagrams and formal specification languages.
- Software Coding Standards - 11.8
 - » ... Software Code Standards ... should include:
 - ... constraints imposed on permitted coding conventions, such as the degree of coupling between software components ...
- Design Description – 11.10
 - » ... a definition of the software architecture and the low-level requirements... This data should include:
 - d. The data flow and control flow of the design.
- Modifications to Previously Developed Software - 12.1.1
 - » The area affected by a change should be determined. This may be done by data flow analysis, control flow analysis, timing analysis and traceability analysis.
- Qualification Criteria for Software Development Tools – 12.2.1
 - » d. Software development tools should be verified... Verification ... may be achieved by:
 - (6) Robustness testing for tools with a complex data flow or control flow, as specified in subparagraph 6.4.2.2, appropriate to the tool's software level.

What About A-7.8?
© Jeff Knickerbocker, 2002

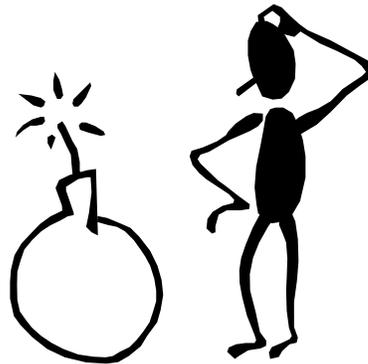
SW DER Conference 2002

3

Analysis, Test, Data Flow, Control Flow, Data Coupling, Control Coupling

- And now we have a problem!
- DO-178B asks for test coverage of data coupling and control coupling (A-7.8)
- DO-178B also asks for data flow and control flow requirements to be recorded in the Design Description (11.10)...
- And what about OO ??!??

SOMETHING SEEMS WRONG !!



What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

4

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Coupling Versus Flow



- Data and control coupling are relational **attributes** that can **only** be analyzed at the design level
- Data and control flow are relational **behaviors** that *may* be *observed* at run time
- So what are you going to test and what are you going to analyze?

Even if DO-178B is not clear in this area, you can still win by thinking...

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

5

More Terminology
(adding precision – we hope)

- And then some inter-module definitions and background...
 - control coupling (*term used and defined*)
 - » *The manner or degree by which one software component influences the execution of another software component.*
 - data coupling (*term used and defined*)
 - » *The dependence of a software component on data not exclusively under the control of that software component.*
 - control flow (*term used but not defined*)
 - » The sequence in which operations are performed during the execution of the computer program. (IEEE Std. 610.12-1990)
 - data flow (*term used but not defined*)
 - » The sequence in which data transfer, use, and transformations are performed during the execution of a computer program. (IEEE Std. 610.12-1990)
 - cohesion (*actually intra-module, not used and not defined*)
 - » The manner and degree to which the tasks performed by a single software module are related to another. (IEEE Std. 610.12-1990)

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

6

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Applying the Concepts



- Let's discuss two fundamental design concepts...
 - Coupling
 - Cohesion
- Just enough discussion to get by, not enough to make a design expert

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

7

Software Component Relationships

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- Coupling (inter-module)

strong	<ul style="list-style-type: none"> - Content Coupling - Common Coupling - Control Coupling » (not DO-178B version) - Stamp Coupling - Data Coupling » (not DO-178B version) - No Coupling 	Weak/ no relationship
--------	---	--------------------------

- Cohesion (intra-module)

not so good	<ul style="list-style-type: none"> - Coincidental - Logical - Temporal - Procedural - Communicational - Sequential - Functional - Informational (OO Concept) 	Weak/ no relationship
-------------	--	--------------------------

best

strong

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

8

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Content Coupling

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- Sometimes called pathological coupling - a type of coupling in which one module affects or depends upon the internal implementation of another (Page-Jones)
- Given two modules M1 and M2, M1 is content coupled to M2 if module M1 makes direct reference to or modifies the contents of module M2
- Not a good practice, but historically this has been done to improve either performance or solve memory problems
- **Can make verification difficult**

Module M1

```
goto L:
.
.
x = a
```

Local Data

```
a: integer
```

Module M2

```
L: .
.
y = x
```

Local Data

```
x: integer
y: integer
```

- M1 branches directly to M2
- M1 modifies local data of M2
- M1 modifies instructions of M2
 - » not depicted
- A calling relationship is not required
- Remove either module M2 and module M1 may no longer be viable
- Modify either module and the other may no longer be viable

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

9

Common Coupling

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A type of coupling characterized by two modules referring to the same global data (Page-Jones)
- Given two modules, M1 and M2, M1 is common coupled to M2 if module M1 and module M2 access the same global data structure with a write-read relationship
- Not a good practice, but historically this has been done to improve performance - it is faster than calling functions
- Not needed to make variables available to test equipment (a write-no read relationship would work for that)
- **Makes regression analysis and re-test a real pain**

Module M1

```
shared_data = value1
```

Module M2

```
value_2 = shared_data
```

The diagram shows a cloud labeled 'Global Data' containing 'shared_data'. An arrow labeled 'write' points from Module M1 to the cloud, and an arrow labeled 'read' points from the cloud to Module M2.

- A calling relationship is not required
- Many modules could be impacted by a global data change (there may be more than two modules in the common coupled set)

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

10

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Control Coupling

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A type of coupling in which one module communicates information to another module for the explicit purpose of influencing the execution of the latter (Page-Jones)
- Given two modules, M1 and M2, M1 is control coupled to M2 if module M1 calls module M2 and an element of control is passed between M1 and M2
 - element of control - a parameter directly influencing the execution of the called module
- **Adds regression analysis and re-test effort - all functions will need impact evaluation and possible re-test.** May wish to break into separate callable units

- A calling relationship is required
- A control element must be passed as a parameter - e.g., function code, flag, switch
- May be difficult to understand - many calls to read_sensors but without knowing FC, it is difficult to determine what function is actually occurring

What About A-7.8?
© Jeff Knickerbocker, 2002

11

SW DER Conference 2002

Stamp Coupling

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A type of coupling characterized by two modules referring to the same composite data structure (Page-Jones)
- Given two modules, M1 and M2, M1 is stamp coupled to M2 if module M1 calls M2 using a data structure as a parameter and module M2 does not access all elements of passed structure
- **Adds regression analysis and re-test effort - all data elements will need impact evaluation and possible re-test** (M2 may inadvertently modify the passed data structure)
- May wish to break up data structures (it depends on the tradeoffs involved)

data_structure
Element 1
Element 2
Element 3
Element 4
Element 5
Element 6
Element 7
Element 8

- A calling relationship is required
- Not all elements of data_structure are utilized by module M2
- Could be either pass by reference or pass by value

What About A-7.8?
© Jeff Knickerbocker, 2002

12

SW DER Conference 2002

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Data Coupling

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A form of coupling in which one module communicates information to another in the form of parameters, each parameter being either a single field or table, each of whose entries hold the same kind of information (Page-Jones)
- Given two modules, M1 and M2, M1 is data coupled to M2 if module M1 calls M2 using a data structure as a parameter and module M2 accesses all elements of passed structure
- Data structure may be simple - e.g., a single variable
- **No doubt about what elements are being set or used. Limits verification scope. Good practice**

```

module M1
  |
  v data_structure
module M2
  data_structure.1 = x
  data_structure.2 = y
  data_structure.3 = z
  data_structure.4 = a
  data_structure.5 = b
  data_structure.6 = c
  data_structure.7 = d
  data_structure.8 = e
    
```

data_structure
Element 1
Element 2
Element 3
Element 4
Element 5
Element 6
Element 7
Element 8

- A calling relationship is required
- All elements of data_structure are utilized by module M2
- Could be either pass by reference or pass by value

What About A-7.8?
© Jeff Knickerbocker, 2002

13

SW DER Conference 2002

Coincidental Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A random grouping of activities (Page-Jones)
- There are no meaningful relationships among the procedural elements in a module
- **Adds regression analysis and re-test effort - all procedural elements will need impact evaluation and possible re-test**
- May wish to break up or reallocate procedural elements

```

module M
  read sensor_inputs
  write arinc_210
  read aircraft_config
  .
  .
  .
    
```

What About A-7.8?
© Jeff Knickerbocker, 2002

14

SW DER Conference 2002

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Logical Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A grouping of activities based on a real or imagined similarity of implementation without regard to data flow, order, time or execution (Page-Jones)
- Implies some meaningful relationships among the procedural elements in a module
- **Adds regression analysis and re-test effort - all procedural elements will need impact evaluation and possible re-test**
- May wish to break up or reallocate procedural elements

```
module read_sensors
  read gyro_inputs
  read accel_inputs
  read adr_inputs
  read isa_temp
  .
  .
  .
```

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

15

Temporal Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A grouping of activities based on time of execution in a particular implementation without regard to data flow or order of execution (Page-Jones)
- All procedural elements are executed together
- **Adds regression analysis and re-test effort - all procedural elements will need impact evaluation and possible re-test**
- May or may not wish to break up or reallocate procedural elements depending on the tradeoffs involved
- Often done for an initialization sequence or for synchronization

```
module initialize_sensor_data

  for i = 1 to 3 do
    gyro_inputs[i] = 0
    accel_inputs[i] = 0
  end for

  isa_temp = 0
  .
  .
  .
```

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

16

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Procedural Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A grouping of activities based on order of execution in a particular implementation without regard to data flow (Page-Jones)
- The module performs a series of related functions
- **Adds regression analysis and re-test effort - all procedural elements will need impact evaluation and possible re-test**
- May or may not wish to break up or reallocate procedural elements depending on the tradeoffs involved
- In this case, data is related but not the same data structure

```
module gnssu_status
    read gnssu_arinc(gnssu_data)
    .
    .
    .
    gnssu_status = gnssu_data.status
    .
    .
    .
    write fms(gnssu_status)
    .
    .
    .
```

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

17

Communicational Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A grouping of activities such that each activity uses the same input data and/or contributes to producing the same output data without regard to order of execution (Page-Jones)
- The module performs a series of functions and the functions access the same data structure
- **Adds regression analysis and re-test effort - all procedural elements will need impact evaluation and possible re-test**
- May or may not wish to break up or reallocate procedural elements depending on the tradeoffs involved
- In this case, "data" is the common data structure and the procedures being executed against the data structure could be executed in any order

```
module process_data
    sum data
    sort data
    report data
    .
    .
    .
```

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

18

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Sequential Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A grouping of activities such that output data produced by one activity serves as input data to another activity (Page-Jones)
- The module performs a series of functions and the output from the previous function becomes an input to the next function
- **Adds regression analysis and re-test effort - all procedural elements will need impact evaluation and possible re-test**
- May or may not wish to break up or reallocate procedural elements depending on the tradeoffs involved
- In this case, "gyro_data" is incrementally processed by each successive function until the gyro rate data is calculated

```
module process_gyro_data
    read gyro_data
    integrate gyro_data
    calculate gyro_rate
    .
    .
    .
```

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

19

Functional Cohesion

(Not DO-178B - Coupling and Cohesion - IEEE & Page-Jones)

- A grouping of activities such that each and every activity contributes to the same single problem-related function (Page-Jones)
- The module performs exactly one function
- **Greatly eases regression analysis and re-test effort - all procedural functions are isolated**
- "Best" type of cohesion for procedural languages
- Contrast with the example for logical cohesion in which the various inputs were read within a common module

```
module read_gyros
    read gyro_inputs
```

```
module read_accels
    read accel_inputs
```

```
module read_adr
    read adr_inputs
```

```
module read_isa
    read isa_temp
```

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

20

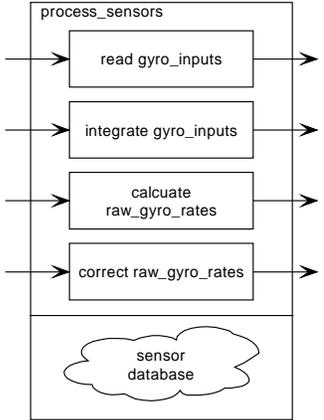
FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Informational Cohesion

(Not DO-178B - Coupling and Cohesion)

- The module performs multiple functions
- Each function is represented by separate entry and exit points (separate methods)
- All functions (methods) access the same data structure
- The data structure is local to the module (hidden in class)
- OO concept - not directly realizable with "C" or Pascal. Very important if re-use is a major issue for an organization
- Nice way to partition problem for verification (or sensor replacement). **Allows stand-alone, requirements based tests on an entire functional block (class)**
- Contrast with the example for sequential cohesion where all the operations were combined in a single module



The diagram illustrates a module named 'process_sensors'. It contains four sequential methods: 'read gyro_inputs', 'integrate gyro_inputs', 'calculate raw_gyro_rates', and 'correct raw_gyro_rates'. Each method has its own input and output arrows. Below these methods is a cloud-shaped box labeled 'sensor database', which is shared by all methods. The entire module is enclosed in a rectangular box.

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

21

OO Specific Considerations

- Speaking of OO...
What could we do for something besides procedural designs?

Many aspects of traditional, procedural coupling, cohesion, and flow techniques may be applied to methods and classes...

But because we combine data and processing in OO designs, we may need to expand our thinking a little bit

Several basic "coupling", "cohesion" and "complexity" methods which could be used with OO analyses activities are presented

Note there are many more techniques in the OO literature not mentioned here...



A black silhouette of a person standing with one hand on their hip and the other scratching their head, with a question mark above their head, symbolizing deep thought or confusion.

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

22

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

OO Indicators – Complexity

(intra-class)

- Weighted Methods per Class (WMC)
 - The WMC is a sum of the complexities of the methods. This can be calculated as follows:
$$\text{WMC} = \sum (\text{method}_n * \text{complexityOfModule}_n)$$
 - **As the number of methods increase and/or the complexity of the methods increase, the greater the potential cost will be in terms of verification effort. This applies to both base classes and sub-classes and impacts verification activity and impact analyses**
- Response for a Class (RFC)
 - The RFC is directly related to overloading and inheritance (more closely related to Dynamic Dispatch). It addresses the cardinality of the set of methods that can be invoked in response to a message and can be calculated as follows:
$$\text{RFC} = \sum (\text{methodInvoked}_n)$$
 - **If RFC is relatively large, verification and change impact analyses may likely be more expensive**

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

23

OO Indicators – Cohesion

(the degree to which methods within a class are related to one another – intra-class)

- Cohesion of Methods (COM) (LCOM is another very similar analysis technique)
 - COM uses data members and methods to assess similarity between methods. Lack of similarity **can help** identify sub-optimal designs and may be calculated in several ways... **One** method is presented below:
$$\text{COM} = (\sum \text{COM}_m) / \text{totalNumberOfDataMembersInClass}$$
 - where
$$\text{COM}_m = (\sum \text{method}_n \text{UsingDataMember}_m) / \text{totalNumberOfMethodsInClass}$$
 - Using this method, a larger value of COM indicates a high level of cohesion ($0 < \text{COM} \leq 1$)
 - A higher value of COM indicates “good” decomposition while low COM values **may** indicate “problems”
 - Classes with low values of COM may benefit from further decomposition
 - **Lack of cohesion may drive increased verification effort and more extensive change impact analyses in the maintenance phase**

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

24

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

OO Indicators – Coupling

(the degree to which objects depend on one another – inter-class)

- Coupling occurs when messages are passed between objects
 - Classes are coupled when methods declared in one class use methods or data members from the other classes
 - Focus on non-inheritance coupling – we will consider something else for inheritance
- Coupling Between Object Classes (CBO)
 - CBO is very simple – we just count the number of distinct, non-inheritance related classes that our class depends on
 - » A smaller number is better than a larger number
 - » If we have a high level of coupling, we **may** want to consider re-architecting our design for more independence (modularity)
 - » As in procedural approaches, the less coupling we have, the more independent (modular) our classes will be
 - **Tight coupling will typically increase verification effort, reduce class reusability, and create more headaches when performing change impact analyses in the maintenance phase**

What About A-7.8?
© Jeff Knickerbocker, 2002

25

SW DER Conference 2002

OO Indicators – Inheritance

(creation of a new class object through the extension of an existing class object)

- Inheritance drives two seemingly inverse relationships
 - Inheritance decreases complexity by reducing the number of operations and operators
 - Excessive inheritance abstraction can make maintenance and subsequent design difficult
 - Since there are two counter attributes, we might want to examine two different indicators...
- Depth of Inheritance Tree (DIT) (corollary to Number of Inherited Methods – NIM)
 - » To calculate DIT we simply count the number of inheritance classes between our current class and the most base class we inherit from ("depth" of our inheritance tree)
 - » The more inheritance levels we have, the harder it may be to determine the behavior of our specific object due to complexity
 - » **A large DIT (> 5) will likely increase verification effort, reduce reuse opportunities, and increase the work associated with change impact analysis in the maintenance phase**
- Number of Children (NOC) (closely related to DIT)
 - » To calculate NOC we count the number of our immediate subclasses
 - » As the number of immediate subclasses increase, we increase the probability of an improper base to subclass relationship (**bad thing**)
 - » Conversely, the more immediate subclasses we have, the more reuse we have achieved (**good thing**)
 - » **A large value of NOC will likely increase verification effort, reduce future reuse opportunities, and increase the work associated with change impact analyses in the maintenance phase**

What About A-7.8?
© Jeff Knickerbocker, 2002

26

SW DER Conference 2002

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?



Be Reasonable,
You Have a Yardstick...

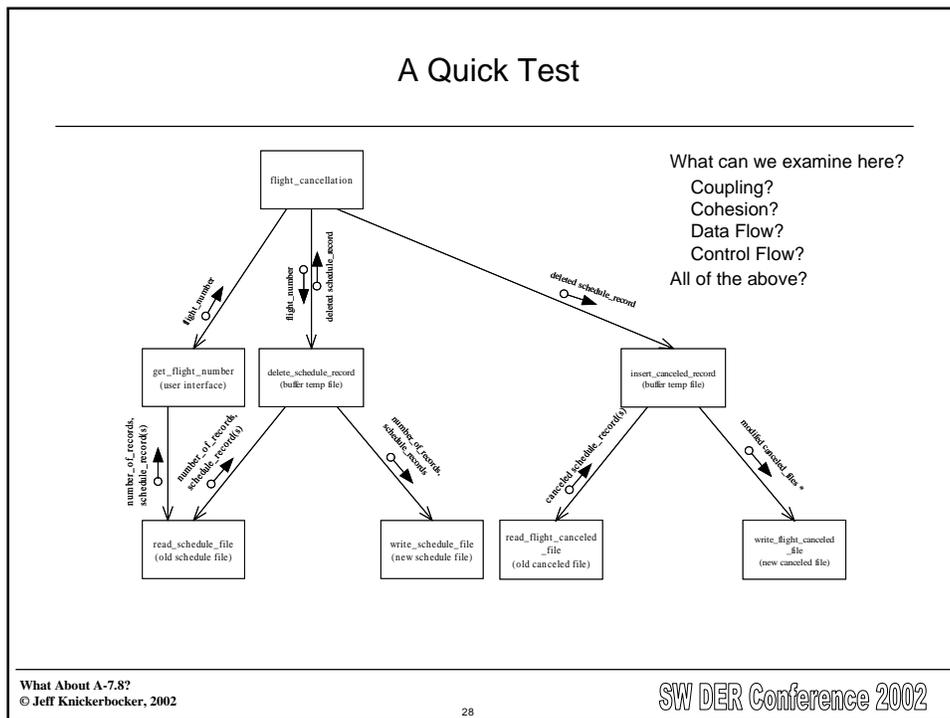


Don't measure with a micro-
meter and cut with an axe!

What About A-7.8?
© Jeff Knickerbocker, 2002

SW DER Conference 2002

27



FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Back to DO-178B Coupling and Flow

- So, after that rather lengthy detour, we are ready to get back to DO-178B...
- What do we now know?
 - It appears DO-178B has generously overloaded the term “control coupling” to refer to
 - » Page-Jones control coupling
 - » Page-Jones content coupling
 - While the DO-178B term “data coupling” refers to
 - » Page-Jones data coupling
 - » Page-Jones stamp coupling
 - » Page-Jones common coupling
 - And there is no DO-178B discussion of cohesion
 - No silver bullets — we make trade-offs
- **Given the ambiguity that has been introduced, we rely on other sources for good design and verification practices**



However, we know A-7.8 is in a set objectives that addresses test coverage analyses!

What About A-7.8?
© Jeff Knickerbocker, 2002

29

SW DER Conference 2002

What did the Committee Want?

- Interviews with knowledgeable SC-167 participants indicate it is very unlikely the committee was after design level coupling and/or cohesion relationships when Table A-7.8 was written!
- “Bugs lurk in corners and congregate at boundaries...”**
- Boris Beizer*
- **In the context of A-7.8, our boundaries may be across inter-function control and data interfaces**
 - **Coupling and cohesion analysis can still help us reduce interface verification work**



What About A-7.8?
© Jeff Knickerbocker, 2002

30

SW DER Conference 2002

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Coupling Versus Flow

- Data Coupling and Control Coupling
 - After considering all the previous points of view with regard to coupling, cohesion and flow, DO-178B is still inescapable...
 - » Objective A-7.8 states,
Test coverage of software structure (data coupling and control coupling) is achieved.
- Because of the ambiguity in the DO-178B definitions, there is significant controversy surrounding verification of data coupling and control coupling
 - Good software engineering practices should prevail, which is to say,
 - » **Analyze & review** the design for good coupling and cohesion practices using IEEE, Page-Jones definitions (procedural) or other well thought out analysis techniques (OO)
 - » **Test** the code using the data flow and control flow requirements as specified in the low level requirements
 - » **Consider** the following interpretation (**not** DO-178B):
Test coverage of software structure (data flow and control flow) is achieved.

What About A-7.8?
© Jeff Knickerbocker, 2002

31

SW DER Conference 2002

Test Coverage of Control and Data Flow

OUCH!

- Who is doing data and control flow testing?
 - Some companies are but...
 - Data flow testing can become very, very complex when taken beyond a simple check of passed parameters...
 - Control flow may not be as difficult, but it would appear to be a type of “white box” test
 - Then of course, there are some questions to be answered...
 - » Static versus dynamic?
 - » Integrated versus unit?
 - » What is the trade-off between static, dynamic, integrated and unit?
 - » Who is the certifying agency?
 - » What are the strengths and weaknesses (vulnerabilities) of your particular implementation choice?
 - **Can your coupling and cohesion analysis help you reduce your data and control flow verification costs?**

What About A-7.8?
© Jeff Knickerbocker, 2002

32

SW DER Conference 2002

FAA National Software Conference, May 2002

Data and Control Coupling: What About A-7.8?

Data and Control Flow Coverage Summary

- There is no BEST way but,
 - » plan, implement, and evaluate continuously
 - » create good design and coding standards and use them
 - » the implementation language and compiler choice may complicate things (pointers, pass-by-reference, pass-by-value, optimization, etc.)
 - » document your approach for A-7.8 in your planning documents – get early certification authority buy-in
 - » communicate, communicate, communicate
- Use talented staff members - expertise in solid software engineering techniques is essential
- Be disciplined and organized - Time spent in design analysis will reap dividends when the final verification package is being prepared
- Develop designs that are testable - Time spent partitioning (partitioning in the sense of weak coupling and strong cohesion) a design (procedures, classes/methods, and data members) will make testing much more efficient while allowing test efforts to be prioritized
 - 1) $\text{system} = \text{function-1} \cup \text{function-2} \cup \dots \cup \text{function-n}$, and
 - 2) $i \neq j \Rightarrow \text{function-i} \cap \text{function-j} = \emptyset$where function_i is composed of both data and procedures
- Use coverage analysis tools against requirements based test cases whenever you can

What About A-7.8?
© Jeff Knickerbocker, 2002

33

SW DER Conference 2002



What About A-7.8?
© Jeff Knickerbocker, 2002

34

SW DER Conference 2002