WG-23 Ada Annex comments -- T. Taft 10/2014

General terminology section:

"Atomic and Volatile" are described as though they are synonyms. The description makes sense for Atomic, but Volatile should be adjusted to conform to the Ada 2012 description. "pragma Volatile" should similarly be adjusted to conform to the new description, which is based more on ordering.

Aspect specification should be added, and explicit mention of "pragma" should generally be generalized to "pragma or aspect specification."

May want to mention the notion of a storage "subpool," which is an Ada 2012 concept.

May want to mention precondition, postcondition, type-invariants, and subtype-predicates, or more generally "assertion expressions."

***Put some wording into general document.***

C.3.2 Guidance

The predefined 'Valid attribute for a given {scalar} subtype ...

C.4.2 Guidance

May want to update "volatile" descriptions, and perhaps use more general "aspect" terminology rather than talking in terms of pragmas.

C.9 Buffer Boundary Violation

There should perhaps be some discussion of user-defined storage pools in the context of buffer overflow, in that a badly designed storage pool could lead to serious problems. Ada 2012 adds storage subpools, which also can produce buffer overflows if not properly managed.

C.15 Dangling Reference to Heap

User-defined Storage Pools and Subpools should probably also be mentioned here, as incorrect management of storage (sub)pools could produce dangling references.

C.31 Loop Control Variables

With generalized iterators, there are new kinds of for loops, so these should be examined for possible vulnerabilities. These may depend on user-written code to properly perform an iteration, so there might be vulnerabilities associated with that.

***Add generalized iterators to main document (new vulnerability?)***

C.34 Passing Parameters and Return Values

Ada 2012 adds some control over aliasing, by using preconditions and the Storage\_Overlaps attribute. This seems relevant to this section, particularly for guidance. Use of Preconditions and Postconditions might also be relevant to this section.

C.41 Memory Leak

Use of Storage Subpools seems relevant to this section

C.45 Argument Passing to Library Functions

Use of Preconditions and Postconditions seems relevant to this section.

C.46 Inter-Language calling

Use of Preconditions and Postconditions seems relevant to this section.

C.48 Library Signature

Use of Preconditions and Postconditions seems relevant to this section.

C.49 Unanticipated Exceptions from Library Routines

Use of Preconditions and Postconditions seems relevant to this section.