

CSI

*How I've come to hate Low/High
Level Requirements*

Mike DeWalt
Certification Services Inc.
Voice 425.228.8712, Fax 425.271.3570
Email: Mike.DeWalt@Certification.com

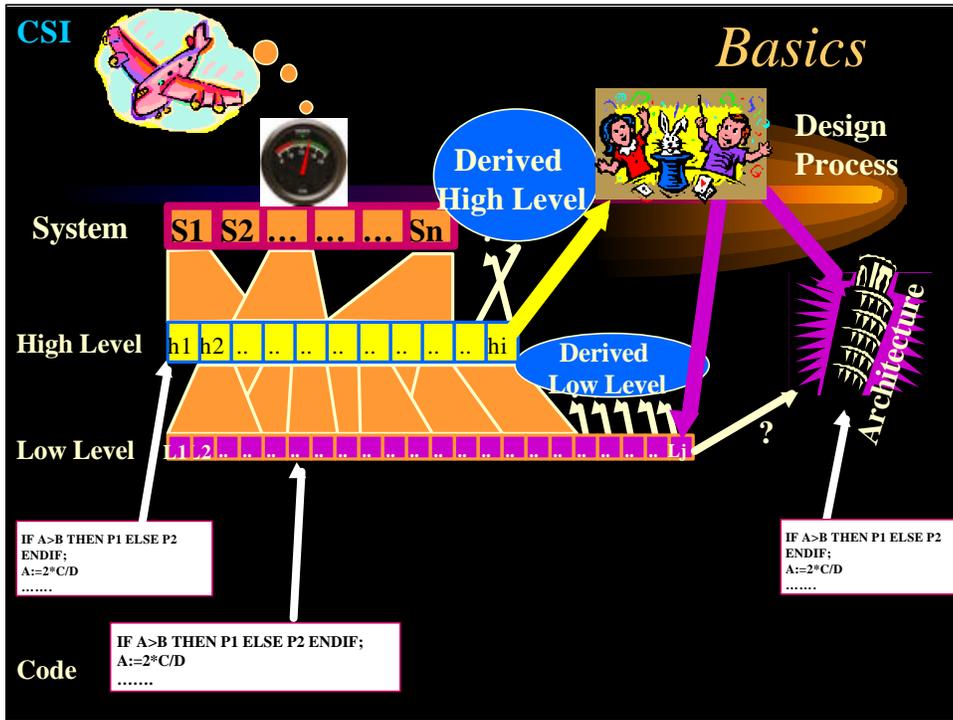


HI

Why worry

- Determination of DO-178B objective applicability
- Subcontractor/Applicant relationships
- Potential for reuse

LOW



Requirements Terminology

- **System** – [Requirements] for a collection of HW & SW components organized ... function(s)
- **High-level** – SW requirements developed from ... system, safety related, and system architecture requirements
- **Low-level** – SW requirements “derived” from high-level requirements, derived requirements, and design constraints ... source code directly implemented w/o further information
- **Architecture** – SW structure to implement SW Requirements (e.g. Invocation (control flow), inter SW component communication (data flow), decomposition

System Requirements: [Requirements] for “A collection of hardware and software components organized to accomplish a specific function or set of functions”

High-level requirements: Software requirements developed from analysis of system requirements, safety-related requirements, and system architecture

Low-level requirements: Software requirements derived from high-level requirements, derived requirements, and design constraints from which source code can be directly implemented without further information.

Software Architecture - The structure of the software selected to implement the software requirements.

Derived Requirements

- General
 - Not **directly** traceable to *higher* level requirements
 - Need to be exposed to the safety analysis
 - Can appear at high-level or low-level requirements
- Derived high-level requirements
 - No champion at the systems requirements level
 - Example: Maintenance SW for product improvement
- Derived low-level requirements
 - No champion at the high-level requirements area
 - Example: Interrupt handling SW, non-required protection/partitioning

DO-178B defines “derived requirements” as “... requirements that are not directly traceable to higher level requirements.” (5.0 Software Development processes) These derived requirements can impact the safety analysis through re-allocation of SW levels, added functionality, etc. As a result, all of these derived requirements need to be fed back safety analysis process to establish their impact. Both high-level and low-level requirements may contain derived requirements. In some military programs, all requirements developed at one level were traced to the requirements at a higher level of abstraction even if they didn’t fit. DO-178B provided the “derived” bucket to recognize that there are requirements that really aren’t directly traceable.

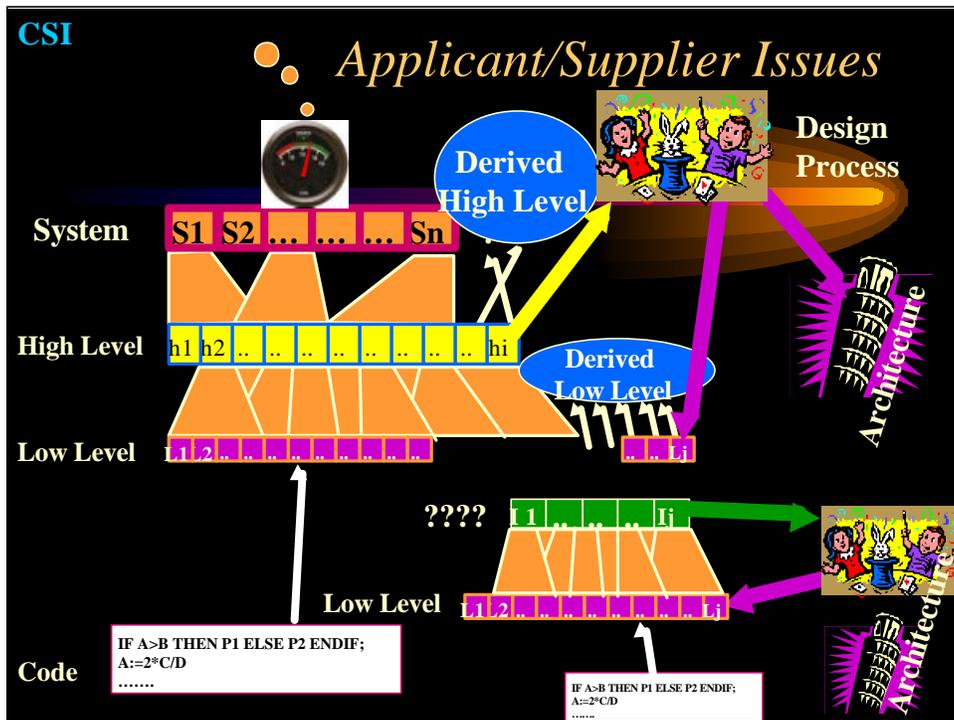
If a high level requirement cannot be traced to a system level requirement then it should be labeled as a derived high level requirement.

An example of such a derived requirement is the need for interrupt handling software to be developed for the chosen target computer.

DO-178B Objective Applicability

- 22 (11 X 2) cover both High & Low Levels:
 - traceability and compliance
 - Verifiability, test coverage, robustness
 - accuracy & consistency
 - standards compliance
 - Definition
- 1 relating to architecture compliance with High Level
- 2 relating to source code and Low Level
- Number of objectives vary from 25 for Level A to 8 for Level D (mostly high level)

Once the Requirements have been categorized into High and Low Level Requirements compliance with the 25 different objectives for Level A is reasonably easy to accomplish.



Applicants have the final responsibility for obtaining approval of software as part of the certification. This usually works its way down to the manufacturer of the Line Replaceable unit where the software is actually executed. When the LRU manufacturer decides to select a supplier for parts of the software the issue of high and low level requirements as well as derived requirements becomes interesting.

The issue boils down to who is responsible for defending the evidences provided to show compliance for the objectives and how that defense is to be mounted.

Applicant/Supplier Issues (cont.)

- Responsibility for compliance demonstration
 - Supplier
 - Manufacturer/applicant
 - Clear definition required
- Traceability
 - Use of derived terminology
 - Renaming by “applicant”
 - Agreement should be generated
- PSAC, SAS, SCID, SECID, +
 - Multiple or single
 - Approval at the applicant level
 - Impacted by low/high level requirements declarations

One way of sorting out the issues is to decide which organization will be responsible for defending the compliance demonstration. If the supplier is the defender then all of their internal processes will be presented to the FAA. This probably results in identifying the interface description between the two organizations as derived high-level requirements. Whereas if the manufacturer/applicant is providing the defense then the supplier is probably being used as subcontract labor and implementing the manufacturers processes and standards. It is very important to make this distinction on an objective by objective basis.

Labeling is important as to establish what activity needs to be accomplished. Where the supplier is providing a “turnkey” package there will probably be low-level and derived high level requirements. In some cases they may be identical for sufficiently low level products such as run time libraries. When integrated by the applicant the requirements will have to be analyzed to determine what the proper label would be in their system.

There are many ways to handle the document submittals depending on the desired relationship between the organizations. This submittal could vary from a complete documentation package including PSACs, SASs etc. to a limited number SW life cycle data items. This will be impacted by the declaration of low-level and high-level requirements.

Potential for Reuse

- Level of approval credit function of high/low level requirements designations
- More explicit definition of remaining effort to complete objectives

One of the most significant issues involved in some of the current projects for reuse have been the definition of high-level and low-level requirements. This impacts the responsibility for objective substantiation and the level of credit that can be claimed by widespread reuse of the project. In order to obtain the desired credit, more careful effort will be required to define any remaining effort for given high-level or low-level objectives at the integration into an applicants product.

Summary

- Affects effort for objective compliance
- Becomes exponentially more important for supplier/applicant relationships.
 - Explicit agreements required
 - PSAC explicit as to who defends objectives
- Additional effort required for general reuse