Assurance Cases for Scientific Computing Software

Spencer Smith, Mojdeh Sayari Nejad and Alan Wassyng

Computing and Software Department, McMaster University

smiths@mcmaster.ca

ASSURANCE cases should be used for certifying Scientific Computing Software (SCS). Benefits for SCS include:

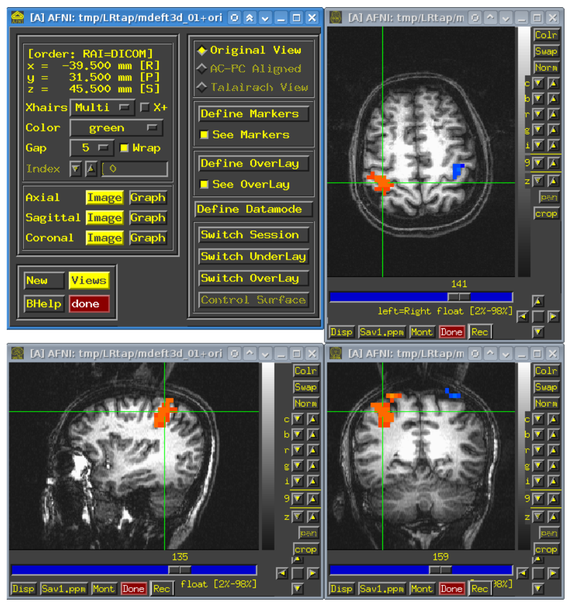
- engaging domain experts
- producing only necessary documentation
- providing evidence that can potentially be verified/replicated by a third party

Assurance case for medical imaging application:

- no errors in the code
- ambiguities and omissions in the documentation
- missing warning about the necessity of using data that matches the assumed parametric statistical model

1. Introduction

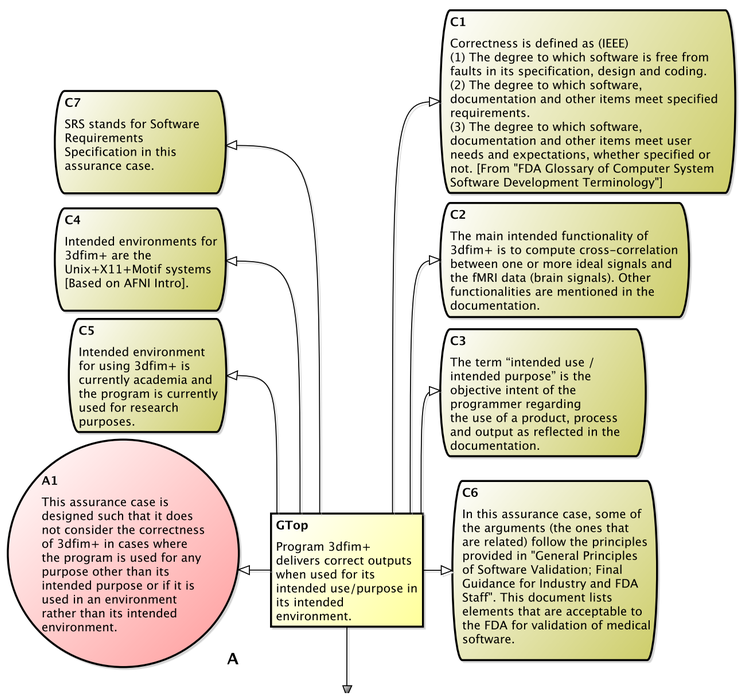
3dfim+ is a tool in the Analysis of Functional NeuroImages (AFNI) package. 3dfim+ analyzes the activity of the brain by computing the correlation between a user-defined ideal signal and the measured brain signal. (Figure from https://commons.wikimedia.org/wiki.)

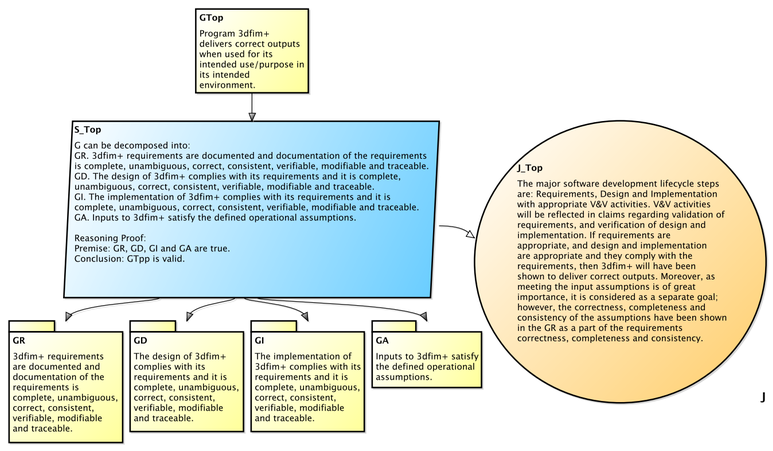


2. Assurance Case for 3dfim+

Top level goal

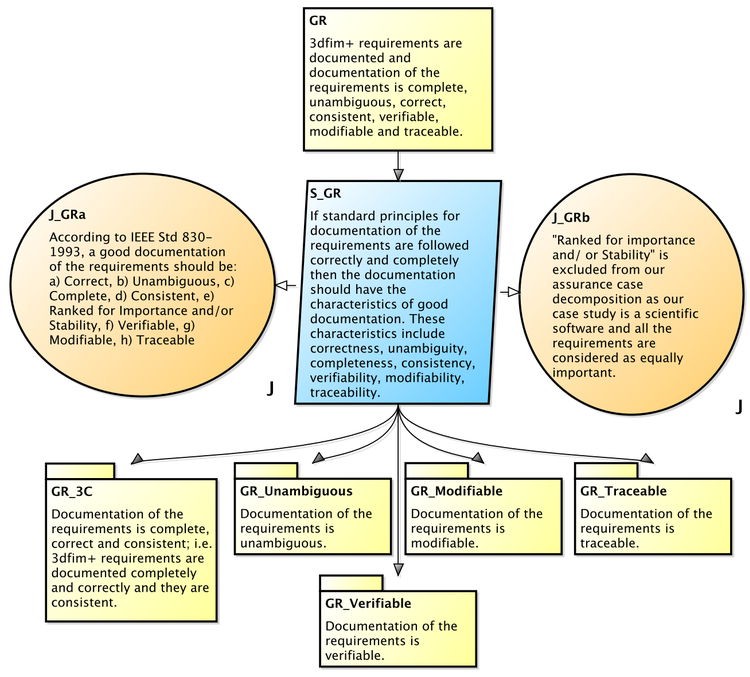
Top goal: "Program 3dfim+ delivers correct outputs when used for its intended use/purpose in its intended environment." The truth of a claim depends on its context.



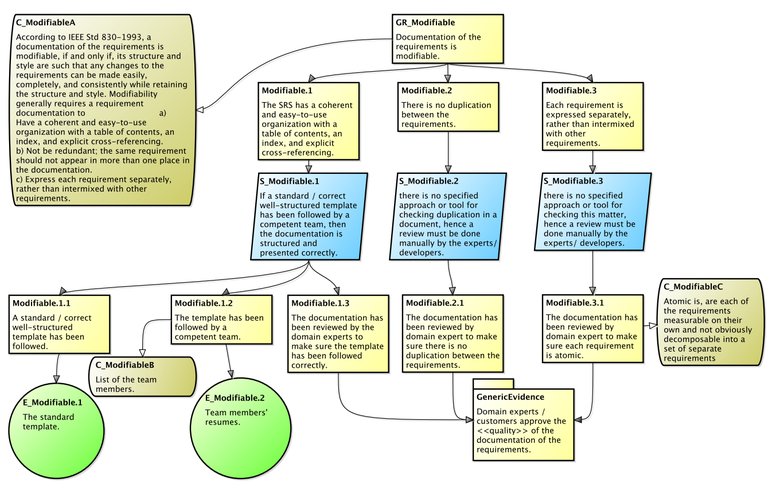


Refine Sub-Goal for Requirements

GR is decomposed into sub-goals based on the IEEE standard 830-1993.

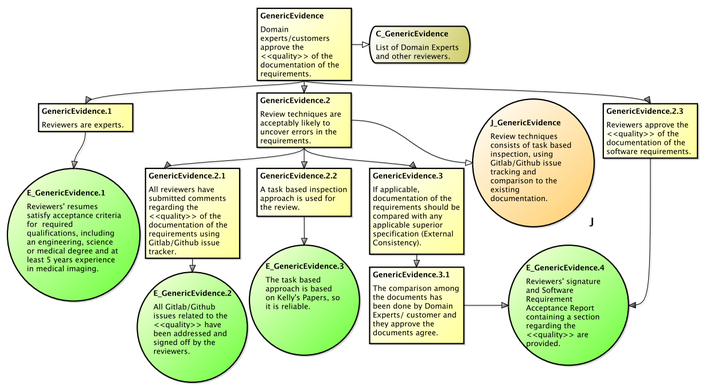


Refine Quality Requirements, like Modifiability



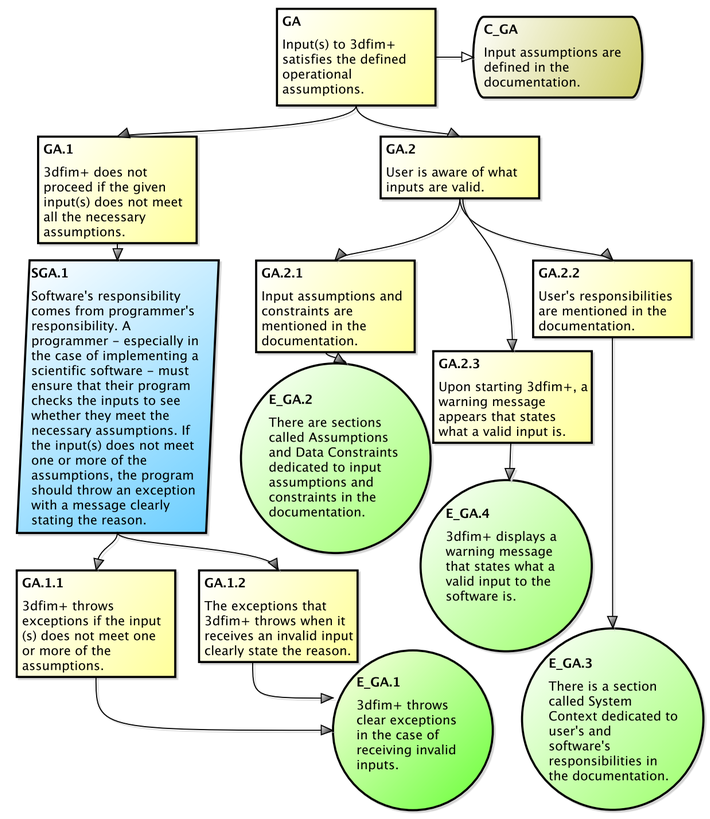
Generic assurance case for qualities

As for the other qualities, the argument for modifiability makes use of a new generic (parameterized) evidence template



Input Satisfies Operational Assumptions

The user has responsibility, in the same sense that an automobile driver has responsibilities to safely operate their vehicle.



3. Removed Ambiguities in Documentation

- Added explicit assumptions (like bivariate normal distribution) and data types (like matrix dimensions) to theoretical model
- Added statement that following Anatomical Coordinate System; original absence led to confusion and multiple test case failures
- Original just said rank function; clarified what to do in the case of ties

$\text{rank}(a, A) : \mathbb{R} \times \mathbb{R}^n \to \mathbb{N}$
$\text{rank}(a, A) \equiv \text{avg}(\text{indexSet}(a, \text{sort}(A)))$

$\text{indexSet}(a, B) : \mathbb{R} \times \mathbb{R}^n \to$ set of $\mathbb{N}$
$\text{indexSet}(a, B) \equiv \{j : \mathbb{N} | j \in [1..|B|] \wedge B_j = a : j\}$

$\text{sort}(A) : \mathbb{R}^n \to \mathbb{R}^n$
$\text{sort}(A) \equiv B : \mathbb{R}^n,$ such that
$\forall(a : \mathbb{R} | a \in A : \exists(b : \mathbb{R} | b \in B : b = a) \wedge \text{count}(a, A) = \text{count}(b, B)) \wedge \forall(i : \mathbb{N} | i \in [1..|A| - 1] : B_i \leq B_{i+1})$

$\text{count}(a, A) : \mathbb{R} \times \mathbb{R}^n \to \mathbb{N}$
$\text{count}(a, A) : +(x : \mathbb{N} | x \in A \wedge x = a : 1)$

$\text{avg}(C) :$ set of $\mathbb{N} \to \mathbb{R}$
$\text{avg}(C) \equiv +(x : \mathbb{N} | x \in C : x)/|C|$

4. Conclusions

ASSURANCE cases for SCS are justified. Although no errors were found in the software outputs from 3dfim+, ambiguities and omissions were found with the original documentation. Running the software does not produce any warning about the obligation of the user to provide data that matches the parametric statistical model. We are currently implicitly trusting SCS developers to build reliable software; the bar should be raised to require developers to create an explicit correctness argument along with their software. Putting the argument in the hands of the experts means that they will find documentation relevant as they work to convince themselves, along with the regulators, of the trustworthiness of their software.

ICSE 2018, 40th International Conference on Software Engineering Companion, May 27-June 3, 2018, Gothenburg, Sweden