Division of Dockets Management
Food and Drug Administration
Department of Health and Human Services
5630 Fishers Lane
Room 1061, HFA-305
Rockville, MD 20852

CITIZEN PETITION FOR MEASURING THE RELIABILITY OF MEDICAL DEVICE SOFTWARE

The undersigned submits this petition under "General Principles of Software Validation; Final Guidance for Industry and FDA Staff" specifically Sec 6.1 of this document entitled, "How Much Validation Evidence is Required?" requesting the Commissioner of Food and Drugs to issue new regulations or amend existing regulations covering measurement of the safety and reliability of software in medical devices.

Present regulations leave everything to the discretion of the medical device manufacturers. The Guidance document(cited above) specifies having systems in place for review by FDA auditors but that results in nothing more than a checklist exercise and lots of wiggle-room for legal extrication from accountability by medical device manufacturers. Further, I contend each of the following documents is similar in this respect ...FDA Quality System Regulations, Medical Device Directive, ISO 13485, ISO 14971, IEC 62366, IEC 62304...

ACTION REQUESTED

To address this issue, I propose the following:

- adopting measurement of code change activity and test activity as the basis for improving software fault management in medical device software

2013-1207

FDA-2013-P-0199

C 1

- manufacturers will then develop an approach that predictably meets release schedules with known safety and reliability, and focus on the organization's business objectives while improving patient outcomes.

STATEMENT OF GROUNDS

The undersigned is personally familiar with applications of measurement technology to software with high reliability and safety requirements where this technology has been proven to be effective.

Software development and testing procedures should be subject to the same rigorous measurement and engineering principles that are standard for hardware systems.

As background, some of the good engineering and mathematics that underlie this approach are presented here < http://www.linkedin.com/redirect?url=http%3A%2F%2Flink%2Espringer%2Ecom%2Farticle%2F10%2E1007%252FBF02249053%3FLI%3Dtrue&urlhash=w5Fb&_t=tracking_disc >

Here's also a link to a slide deck, derived from the Springer link above, that attempts to flesh out the measurement approach...

https://www.dropbox.com/s/g4pupp7ffrbvc0f/Software_Fault_Management.ppt

****

As an example, here's my analysis of a recent Class I recall of a medical device...
http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm338789.htm

Presumably we can agree that having any life-threatening Class1 recalls necessitates some investigation of why and how such recalls occur and could be prevented?

How could 1) measurement of change activity in the static domain, 2) measurement of test activity in the dynamic domain and 3) measurement of the size and character of software faults supplement/complement the discovery(prior to release) of the software faults responsible for the oxygen miscalculation...?

In the context of the FDA's current approach...
* is the software doing what it's supposed to do...?

Answer:
I believe the software is NOT doing what it is supposed to do. In fact there is a fault(s) in the software, such fault(s) having been introduced in architecture, design, implementation... Indeed, faults are introduced by people making errors for very predictable reasons.

As stated previously, FDA/industry need to deal with how med device software fails, i.e., the 'physics' of software failure. And the IEEE Computer Soc already provides a well-thought-out taxonomy of errors>faults>failures as a starting point.

What is important is that unexamined code permitted the fault(s) to remain. Static analysis would have provided direct information on where code problems were likely to be. Inspections and reviews could then have been focused on these areas. You gotta remember the story of the drunk who was looking for his keys around the light post.

Again, in the context of the FDA's current approach...
* parameters entered into the executable code result result in a specific subset of problems that can be life threatening. This is classified as a software failure, and a fix is being delivered.

Answer:
There may be a latent fault(s) in the code that persists for many years. When there is a nuanced shift in the operational profile, the fault may then be expressed and be seen as a failure.

Since the recall extends to "...software versions 1.1.2 and lower." ...this software fault has presumably existed in the code since release 0.0.0 ...

or

It was introduced in some version prior to 1.1.2 --

If measurement of change activity was in place, the vendor would have been able to isolate the precise version where the faulty code responsible for the oxygen miscalculation was introduced... if this were the case it would simplify and reduce the economic impact of the recall considerably.

If we knew the version where the fault(s) we introduced we'd have a chance to ask the developer(s) what was in his/her mind during the process of implementing the design. If this implementation followed the design and was correct... then we could move to the designer(s) and ask again what was in his/her mind in writing the specification describing the design and so on...

In this way, after the fact, we could isolate the root cause.

If indeed the fault(s) causing the oxygen miscalculation were present since version 0.0.0 then this may be a case where the design is faulty... then one would have to ask why since presumably the software went thru the 'paperwork exercise' of '...FDA Quality System Regulations, Medical Device Directive, ISO 13485, ISO 14971, IEC 62366, IEC 62304...' this software fault still escaped to be discovered by a patient(s)?

A design question is why the software isn't designed to fail-safe, i.e., in a non life-threatening way?

Lastly, in the context of the FDA's current approach...
* is this something addressed by our use of the term "software reliability"?

My whole point in this discussion is that none of what I've described above in my answer can proceed without measurement.

Having the FDA mandate installation of a measurement protocol akin to what I've described would effectively prevent such faults from ever being introduced again.

Measuring faults(architecture, design, implementation) is a learn-as-you-go process, i.e., we start out developing measures for those types of faults we've discovered initially(#3 above). With this, we know what to look for in successive builds(#1 above). However, this is still one hand clapping.

As time proceeds and thru knowing what the tests are covering in the code(#2 above), we'll discover still more, as yet unfamiliar faults, that we must fix and also learn to measure(#3 above). This is two hands clapping.

For the O2 miscalculation fault above, if it is ultimately determined to be an implmentation fault then we should learn how to measure it and look for other places in the code where data structures exhibiting similar measurements might also exist.

If the fault is determined to be a design fault then must implement measurements in the design verification testing.

Lets always remember:

Faults throughout the development life-cycle are introduced by people. Likewise, we have a number of techniques, described above(and mandated by the FDA) for removing such faults. The question arises who's going to win this competition between fault introduction and fault removal.

We won't know unless we measure... so let's stop acting like the drunk looking for his keys only under the nearest light post.

ENVIRONMENTAL IMPACT

To the best of my knowledge and belief there is no environmental impact.

CERTIFICATION

The undersigned certifies that, to the best knowledge and belief of the undersigned, this petition includes all information and views on which the petition relies, and that it includes representative data and information known to the petitioner which are unfavorable to the petition.

(Signature) (2/11/2013)

[redacted]

Exemption 6

[redacted] exemption 6

Division of Dockets Mgmt.
Food and Drug Admin.
Dept. of Health and Human Services
5630 Fishers Lane
Room 1061, HFA-305
Rockville, MD 20852

ATTN: Yatta Yarjah