SoftQuest Systems
assuring quality projects

June 30, 2017

Software in Medical Devices – Update for Q1/Q2 2017

This is a continuation of the software updates I have been sending out. Please check out all of the references to download and/or to purchase. If you have any questions, please contact us.

FDA Responses to 510K - Software

Numerous companies have received generic responses from the FDA concerning their software testing (what we would call unit and integration testing). The wording received from the FDA in all of the cases is shown below:

> The submission did not include information on the tools, such as static analysis tools, that you used to detect run-time errors. This information is needed to assess whether good coding practices have been implemented to prevent common coding errors which may adversely affect the safety of the device. Please provide this information. For any such tool used, please identify what error types the tool detects, your method and process of applying the tool(s), and a summary report and/or conclusion about the results. Note: some common run-time errors are:
>
> a. Un-initialized variables
> b. Type mismatches
> c. Memory leaks
> d. Buffer over/under flow
> e. Dead and unreachable code
> f. Memory/heap corruption
> g. Unexpected termination
> h. Non-terminating loops
> i. Dangerous Functions Cast
> j. Illegal manipulation of pointers
> k. Division by zero
> l. Race conditions

We are highly recommending to all clients the following remediation for the information on testing tools during the development:

For all SSC Class B (Moderate LOC) software, we are starting to require tools to test the software for run-time errors. We are recommending using static code analysis tools. There are low end tools that should be used, e.g., Source Code Analysis package for medical device companies from Parasoft (C/C++, C#/VB.NET, Java), Microsoft Visual Studio 2013 Static Code Analysis (C/C++), IAR C-STAT static analysis (C/C++), etc.

2. FDA Responses to 510K - Software

Also, these companies have received generic responses from the FDA concerning their cybersecurity. The wording received from the FDA in all of the cases is shown below:

The information security and cybersecurity of the device is needed to evaluate the cybersecurity risks and the associated controls.

a. Please discuss in detail, information on your design considerations, including mitigations pertaining to intentional and unintentional cybersecurity risks including:
b. A specific list of all cybersecurity risks that were considered in your design.
c. A specific list and justification for all cybersecurity controls that you established, and the justification as to why such controls are adequate. Please provide the evidence that the controls perform as intended.
d. Please ensure that you address information confidentiality, integrity and availability.
e. Please incorporate, as appropriate, the information identified here in your Hazard Analysis.

We are recommending to all clients the following remediation for the cybersecurity:

A cybersecurity report should be prepared for submission to the FDA based upon the threat analysis. This should be done with the emphasis on patient safety and privacy. This does not have to be an elaborate document, but it should cover the main issues.

IEC TR 80002-2

IEC TR 80002-2 Medical device software - Part 2: Validation of software for medical device quality systems has been published. This technical report provides guidance for new requirements in ISO 13485:2016 for validating software used in quality systems. ISO/TR 80002-2:2017 applies to any software used in device design, testing, component acceptance, manufacturing, labelling, packaging, distribution and complaint handling or to automate any other aspect of a medical device quality system as described in ISO 13485. This technical report can be purchased from ISO, IEC, etc.

Implantable Device FDA Cybersecurity Notice

On 10/1/17 the FDA issued a safety notice for the Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter. The FDA has reviewed information concerning potential cybersecurity vulnerabilities associated with St. Jude Medical's Merlin@home Transmitter and has confirmed that these vulnerabilities, if exploited, could allow an unauthorized user, i.e., someone other than the patient's physician, to remotely access a patient's RF-enabled implanted cardiac device by altering the Merlin@home Transmitter. The altered Merlin@home Transmitter could then be used to modify programming commands to the implanted device, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks.

ISO 13485:2016 and Software Validation

The requirements to validate all quality systems (ERP, PLM, PDM, etc.), production systems, measurement systems and service systems have been issued in the ISO 13485:2016 over a year ago. The deadline for implementation is early next year. These validations take time and organizations should not put this off till the last minute.

Software Recalls Q1-Q2 /2017

We have been following the recalls and there were a growing number of recalls that are listed where software played a role in the recall. The following are additional examples of recalls involving software directly as listed on the FDA website. There were over 100 recalls in this period relating to software, including 5 class I recalls (as compared to 3 in the last period). There may be more but classified not under software directly.

1) **Alaris Syringe Pump Module Class I –** CareFusion is recalling the Alaris Syringe Pump because of a faulty Air-In-Line (AIL) sensor which may generate a false alarm, and cause the syringe pump to stop supplying the infusion to the patient. If the AIL sensor is faulty, the false alarm may be

repeated and require the health care provider to clear the alarm to restart the infusion. Interruption of infusion could lead to serious adverse health consequences or death.

2) **Medtronic SynchroMed Infusion System Class I –** Medtronic is following up to a May 2013 communication regarding the Priming Bolus function for the SynchroMed Infusion System. Medtronic is updating the Model 8870 software application card (to version AAU01) and the SynchroMed Infusion System.
3) **LIFEPAK 1000 defibrillator Class I –** The firm has received complaints that the LIFEPAK 1000 Defibrillator is unexpectedly powering off during device usage.
4) **Newport HT70 & Newport HT70 Plus Ventilators Class I –** Newport Medical Instruments Inc. now a part of Medtronic, is recalling the Newport HT70 and Newport HT70 Plus ventilators because a software problem may cause the ventilator to shut down unexpectedly without sounding an alarm. If the ventilator shuts down, the patient may not receive enough oxygen and could suffer serious adverse health consequences such as brain damage, or even death.
5) **HeartMate II LVS Controller Class I –** Patients may sometimes need to change to their backup back-up system controller during the course of ventricular assist therapy. The change should be done quickly and in the hospital, because it can present a significant challenge to patients that are elderly and/or untrained. For these patients, a slow or improper driveline changeover places them at risk of serious injury or death. Abbott-Thoratec has received a total of 70 reports of incidents in which the controller has malfunctioned after an exchange, including 19 injuries and 26 deaths. All of the deaths occurred when patients attempted to exchange controllers while away from the hospital. To address this issue, Abbott-Thoratec is providing all HeartMate II LVAS with Pocket Controller users with new software and hardware updates to assist patients in successfully changing their pocket controller in emergency situations.
6) **Merge DR Systems Unity Class II –** The software fails to associate to the correct MG image if there are two images for the same view.
7) **Toshiba Ultimax DREX-ULT80,0 Class II –** It has been found that the generator of the system could possibly terminate the exposure prematurely during an examination. This issue was identified due to a software problem residing in the generator firmware.
8) **Siemens Artis zee/zeego Class II –** Siemens initiated a corrective action to address two possible, mutually independent causes of a system defect related to the following: - In Artis Systems with A100 Plus or A100G generators, an attempt to resume operation following detection of a fault can result in the failure of a module in the high-voltage generator.

9) **Philips IQon Spectral CT Class II –** Multiple issues have caused the device to result in CT rescans or incorrect scan location or misrepresentation of image results.
10) **Elekta Oncentra External Beam Class II –** Cross profile for Varian 60 degree wedge shows "horns."
11) **Elekta Monaco RTP System Class II –** Incorrect Enhanced Dynamic Wedge (EDW) or Virtual Wedge (VW) Calculations.
12) **Eclipse Treatment Planning System Class II –** Modifications in version 13.6MR2 for Contouring, SmartAdapt, and SmartSegmentation workspaces resulted in contours not being saved consistently in Eclipse. Treatment Planning System. The issue only occurs if certain conditions are fulfilled.
13) **Fresenius 2008 Series Hemodialysis Systems Class II –** When the UF Rate, Goal or Time is adjusted using the up and down arrow keys, and the change is cancelled by using the esc key, the cancelled UF Rate is actually being executed rather than rate displayed on the machine.
14) **Digital RID Plate Reader Class II –** If a control ring is marked after reading, the software will not flag results that are out of the specified QC range.
15) **Carestream Touch Prime Class II –** Software error; Carestream Health Inc, received a complaint stating that when a user accidentally obtains a measurement value of 0 and corrects the value in the report, the resulting measurement unit is not displayed, i.e., centimeters or millimeters. As such, the user expects that the measurement is taken calculated in centimeters, consistent with other values in the report. In actuality, the measurement is taken in millimeters. When this updated measurement is used in an average calculation, the result appears incorrect as two measurements are interpreted as centimeters while the user corrected value is interpreted as millimeters. If the user selects a Calc Result display as Min or Max, the values are also interpreted as millimeters when centimeters were expected.
16) **Blood Bank Control System (BBCS) Class II –** Blood Bank Control System (BBCS) with Primary Application (software version BBCS Primary Application 5.4.3, 5.5; ABO Express 1.0.0, 1.1.0, 1.2.0), with a defect or glitch, was distributed.
17) **Ambra PACS UDI Class II –** A software error caused the window/level to become the same in one series regardless if the image had different levels; image results have a washed-out grey appearance.
18) **SCC Soft Computer Softbank software Class II –** Software error. Potential for incorrect results.
19) **Roche Cobas b 123 POC system Class II –** Under specific settings, an issue may occur during simultaneous Sensor Cartridge and Fluid Pack change on the cobas b 123 <2> POC system and cobas b 123 <4> POC system. The issue occurs when the software function [AutoQC as follow-up] is configured to run all three levels of AutoQC only after a Fluid Pack change, but not after a

Sensor Cartridge change. When both are changed simultaneously, starting with the Sensor Cartridge and followed by the Fluid Pack, the analyzer carries out only the follow-up actions associated with the Sensor Cartridge change after completing the change workflow. As a result, no follow-up AutoQC is performed and the three expected AutoQC measurements for the Fluid Pack change are not carried out. Without running quality control, there is a remote possibility that system issues would not be detected and wrong results would not be excluded on all parameters: pH, PO2, PCO2, Na+, K+, Ca++, Cl-, Glu, Lac, Hct, SO2, O2Hb, COHb, MetHb, HHb, and Bili.

20) **Roche Accu-Chek App Class II –** iOS and Android: Under certain conditions the affected app versions may disregard historical bolus data potentially leading to an incorrect bolus insulin recommendation being provided to the user. iOS only: Pairing and using multiple meters with the Accu-Chek Connect app can under rare circumstances cause the bolus advisor to fail to offer a correction bolus recommendation within the eligible time window following a blood glucose measurement (10 15 minutes). Depending on the individual metabolic situation potentially incorrect bolus advice could lead to serious health consequences such as hypoglycemia. Both software issues may also cause the amount of active insulin displayed during the bolus calculation process to be incorrect and should not be used to manually calculate a bolus.
21) **Merge Hemo software Class II –** The application may crash during the cath lab procedure.
22) **SiemensSyngo.plaza Class II –** Software update for improvements and to resolve several issues.
23) **Siemens Mammomat Inspiration Class II –** Software error.
24) **MEVION S250-Proton Radiation Therapy Class II –** An error can occur causing Delta corrections to be lost when one setup field is closed and another is opened.
25) **Merge RadSuite software Class II –** The values provided from the Pixel Value tool do not appear to be correct, which may result in potential patient injury or delay in diagnosis or treatment.
26) **Merge PACS software Class II –** Potential exists for an incorrect patient image being displayed which could result in the delay in diagnosis or treatment.
27) **Merge Eye Station Class II –** This recall has been initiated due to an issue related to the potential accidental deletion of record(s) by an Eye Station user.
28) **LIFEPAK 15 Monitor/Defibrillator Class II –** The End-Tidal CO2 (EtCO2) reading can intermittently show a value of XXX after start-up or during device operation.

29) **Boston Scientific, EMBLEM S-ICD Programmer Class II –** There is a potential for radio frequency (RF) interference to alter wireless communication from a programmer, which in rare instances may cause an S-ICD to perform an unintended command. This behavior can only occur during an active, in-clinic interrogation/programming session with the Model 3200 S-ICD programmer. There is no risk of this behavior occurring when the LATITUDE Patient Management System communicates with an S-ICD in an ambulatory setting.
30) **VIDAS 3 software v. 1.1.4 Cl II –** During development of the VIDAS 3 software version 1.2, some anomalies have been identified and observed to be already present in the current software version VIDAS 3 version 1.1.4. available in the field.
31) **Siemens CentraLink Data Management System SW Class II –** There is a remote possibility CentraLink may download an order to the ADVIA Automation System without specifying the sample type. This can occur when an order is received from the LIS without a sample type, requiring that the sample type be set in CentraLink based on the sample type of the test in the order.
32) **Philips Efficia CMS200 Class II –** The monitor may not alarm appropriately for a pediatric or neonatal patient.
33) **Merge Eye Station Import Utility (ESIU) Class II –** Eye Station images were not importing properly and were imported under "unknown" due to an issue when validating patients using only an Medical Record Number (MRN).
34) **Keyspan High-High Speed USB to Serial Adap Class II –** Power outages causes reporting software to shutdown.
35) **McKesson Radiology 12.2 - PACS Class II –** Issue for customers that use an EMR login or legacy web URL login or legacy web URL login for McKesson Radiology PACS that may result in missing images in a newly imported study, and/or study imports that remain in an "in-progress" status.
36) **Merge Cardio software using EchoIMS Class II –** A situation can occur allowing two physicians to access the same study report in EchoIMS when launched from the Cardio Study List without receiving the read-only notification prompt.
37) **PhilipsBrightView Class II –** Four issues: 1. Motion controller problem stops scan and no data image produced. 2. Door interlock switch problem disables CT scan. 3. Detector contacts head holder when performing Patient Unload. 4. JETStream freezes during gated planar scan.
38) **Merge Hemo software Class II –** Use of the software may show an incorrect value to the user when viewing the Fractional Flow Reserve (FFR) results during recording.

39) **Arial Wireless Water-Resistant Call Pendant Class II –** Devices were incorrectly programmed during manufacturing therefore depressing the pendant button may result in an alarm not sounding as intended.
40) **Philips V60 Ventilator Class II –** The V60 Ventilator with Version 2.20 software installed may falsely detect that the blower motor has stalled. If this condition occurs, the software will cause the ventilator to shut down (Vent Inop) and display Error Code 100E. Ventilatory support will cease.

Were these software recalls due to insufficient testing? Were they due to not following the SDLC Procedure? Your guess is as good as mine.

Warning Letters

1) **Sato Yakuhin Kogyo Co., Ltd. -** Your firm failed to ensure that laboratory records include complete data derived from all tests necessary to assure compliance with established specifications and standards. Reliance on incomplete data . . . . . .

2) **FACTA Farmaceutici S.p.A Ltd. -** Your firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards. For multiple sterile drug product lots, your original data showed failing results, but data you reported showed passing results. . . . .

3) **Morton Grove Pharmaceuticals, Inc. –** Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records. Your quality system does not adequately ensure the accuracy and integrity of data to support the safety, effectiveness, and quality of the drugs you manufacture. . . . .

4) **Denttio, Inc. –** Failure to perform device software validation and risk analysis as required by 21 CFR 820.30(g). For example, you do not have records to demonstrate that your Imaging Software used with the Tio-H Digital X-Ray Sensor has been validated. You do not have records to demonstrate that your firm has conducted a risk analysis to identify potential hazards and control measures with the Tio-H Digital X-Ray Sensor System.

5) **USV Private Limited –** Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records. . . . .

6) **Mylan Pharmaceuticals, Inc. –** Your firm failed to establish an adequate quality control unit with the authority to review production records to assure that no errors have occurred or, if errors have occurred, that they have been fully investigated. . . . . .

Use of Electronic Records and Electronic Signatures in Clinical Investigations

The FDA released the draft guidance of questions and answers for the "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11". This was sponsored by CDRH, CDER and CBER.

https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM563785.pdf

Personal Information Definition

Three US states have joined others to expand personal information definition to include usernames or email addresses.

General Data Protection Regulation

By the end of May 2018 all hardware and software that processes personal data concerning the health of EU citizens must comply with the General Data Protection Regulation (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016).

Many medical devices record real-time data that, when uploaded to a doctor along with a patient name or other type of patient identifier, become Protected Health Information (PHI) that is governed in the United States by HIPAA. Even if this data is not uploaded to a healthcare provider and PHI is present on the medical device, the design of the medical device must be such that it is not possible to access the PHI through wireless networks, or through hacking into the device or associated software or databases should the device become lost or stolen.

In addition to confidentiality considerations, the MDD requires all risks be reduced as far as possible. In practice, this means that designs are consistent with the generally accepted state-of-the-art and compliant with international standards. If threats to the integrity or availability of data could lead to patient harm, then they must be addressed. This means the application of a systematic, risk based approach to information security as covered by ISO 27001.

<u>21st Century Cures Act</u>

Section 3060. Clarifying Medical Software Regulation. There has been a great deal of uncertainty about the degree to which FDA can and should regulate standalone medical software. This type of software is steadily increasing in importance and capability. This provision modifies the definition of a "device" to remove several categories of software from the FDA's jurisdiction. The categories of software removed from the device definition are:

A. Software that provides administrative support of a healthcare facility. This is non-controversial and arguably was never subject to the device definition in the first place.

B. Software for maintaining or encouraging a healthy lifestyle, and not related to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition. This is non-controversial and is consistent with FDA's General Wellness and Mobile Medical Applications guidance documents.

C. Software that serves as electronic patient records, provided (among other things) that such function is not intended to interpret or analyze patient data or images for the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition. This codifies policy already implemented by FDA as a matter of enforcement discretion.

D. Software for transferring, storing, converting formats, or displaying data/results and associated findings by a healthcare professional (e.g., medical device data systems (MDDS)), unless intended to interpret or analyze the data, results or findings. This codifies FDA's exemption of MDDS technology from regulation.

E. Software for: (i) displaying, analyzing, or printing medical information about a patient or other medical information (such as practice guidelines); (ii) supporting or providing recommendations to a healthcare professional (i.e., clinical decision support) about prevention, diagnosis or treatment of a disease or condition, AND (iii) enabling the health professional to independently review the basis for such recommendations rather than primarily rely on it when making diagnostic and treatment decisions. There is an exclusion for medical images, signals from in vitro diagnostic devices and signals or patterns from signal acquisition systems, i.e., they are not part of this carve out from the definition of a medical device.

IEC 82304

Although IEC 82304-1 Health Software: General requirements for safety has been published, it is not clear when it will be harmonized in the EU. Nonetheless, it appears that the EU notified bodies are treating it as “state-of-the-art” and are likely to expect it to be used for software products that are regulated as medical devices.

IEC 80001-2-9

IEC 80001-2-9, Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities 80001-2-9 has been published. This TR shows how a security assurance case can be used to demonstrate confidence that 80001-2-2 security capabilities have been achieved. This is the latest if the guidances in the IEC 80001 series.

FDA FINAL Guidance Benefit-Risk IDE Devices

The FDA on 13/1/17 issued the final guidance entitled: "Factors to Consider When Making Benefit-Risk Determinations for Medical Device Investigational Device Exemptions". This guidance references software features in Appendix C the device description section. The full guidance is at the link provided.

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM451440.pdf

FDA Draft Medical Device Product Communications

The FDA issued on 21/1/17 a draft guidance "Medical Product Communications That Are Consistent With the FDA-Required Labeling — Questions and Answers". The full draft is at the link provided.

http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM537130.pdf

FDA Postmarket Cybersecurity Guidance Webinar

FDA issued on 12/1/17 the final guidance entitled: “Postmarket Management of Cybersecurity in Medical Devices”. Information and presentation materials are at the link provided.

http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm534592.htm

China FDA (CFDA) - ISO/IEC 14764 for IT maintenance

The China FDA (CFDA) formerly the State FDA (SFDA) maintains an English version of its website at the link provided. The CFDA is promoting use of 62304 for medical device software and essentially ISO/IEC 14764 for IT maintenance. It is also actively expanding its requirements related to cybersecurity of networked devices.

http://eng.sfda.gov.cn

Summary

There are many ways to screw up your software in the medical device. It doesn’t take too much talent. Many companies mess up royally.

You can work properly without breaking the bank. There are many ways to handle the software development/maintenance life cycle and the software validation.

As the software situation (requirements from the regulatory authorities) will only becoming more stringent, we recommend you understand what is needed, how to implement it and do it correctly. Get yourselves the proper help (internal, external, etc.) and do what is needed.

Remember, in most companies there is never time to do a software project correctly, but there is always time to do it 5 or 6 times over.

If there are any questions or requests, please feel free to contact us.

Mike