SoftQuest Systems
assuring quality projects

February 5, 2015

Software in Medical Devices – Update

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.

Software Recalls 2014/2015

Last update we noted the FDA report and recalls for the end of 2014/beginning of 2015. 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:

1) **Covidien Puritan Bennett 980 Ventilator, Class I** - A software issue may lead to ventilator inoperative situations.
2) **VITROS 5600 Integrated System, Cl II -** Ortho Clinical Diagnostics (OCD) identified an anomaly with Software Version 3.0 and below on the VITROS 4600 Chemistry Systems and VITROS Integrated Systems. Internal testing confirmed that when using calibrator barcode labels supplied with VITROS Chemistry Products Calibrator Kits 1, 2, 3, 4, 6, or 9, an unexpected assay calibration may occur if assay targets are unassigned (i.e., hidden).
3) **eFilm Workstation 4.0 and 4.0.1m, Cl II** - There is an issue related to eFilm Workstation versions 4.0 and 4.0.1 when having multiple studies open and utilizing the thumbnail panel to select multiple series from multiple studies may lead to the selection of an incorrect study.
4) **Philips IntelliVue Monitors, Cl II** - Philips Intellivue and Avalon Fetal Monitors in time-synchronized automatic/sequence mode, the NBP automatic measurement series is stopped.
5) **Mindray V21, Cl II -** issue with the V-Series Drug Calculator function.
6) **Merge Hemo Programmable diagnostic computer Cl II** – During use, the SpO2 value displayed on the Hemo Monitor may not update to reflect changes in the patient's oxygen value. It is also possible that if using the pulse rate of the SpO2 finger clip to calculate the patient's heart rate, it too may be subject to displaying a stale value.
7) **Iba Dosimetry Gmbh COMPASS, Cl II** - Error in the software. A deviation between reconstructed and planned dose distribution may not be detected prior to treatment and this can result in an over or under-estimation of the pretreatment delivered dose.

8) **Access 2 Immunoassay Systems, Cl II** - it may experience a "MFC Exception" error during normal operation of the Access 2 Immunoassay Systems.
9) **Philips Allura Xper FD20C, Cl II** - a problem in the Power On Self Test (POST) error handling was detected, can result in a hazardous movement of the C-arc. system.
10) **Maquet Cardiohelp-I System, Cl II** - may have a software issue that can potentially result in an erroneous display of a "Battery Needs Service" message after startup of the units when using either AC or DC power.
11) **Integra Licox Pt02 Monitor, Cl II -** complaints that the USB port on the Licox Pt02 monitor does not consistently provide the user the ability to extract the Pt02 trend data according to the User's Manual for the device.
12) **Elekta MOSAIQ Product Usage, Cl II -** A problem can exist in MOSAIQ resulting in the display of incorrect numeric data due to a dose rounding error on printed reports.
13) **CyberKnife Robotic Radiosurgery System, Cl II** - Software upgrade to correct potential safety issue related to CyberKnife System that occurs when upgrading the Treatment Delivery Software for the first generation Iris Variable Aperture Collimator.
14) **Toshiba Cardiac Function Analysis Software, Cl II -** a potential problem with the cardiac function analysis software (CFA). It has been found that, due to the problem with the software, incorrect analysis results may be displayed in the Function Parameters for the Entire Heart displayed as analysis results of the CFA and in a Left-Ventricular Volume Curve generated based on some of those parameters.
15) **Philips IntelliSpace Portal DX/HX/EX, Cl II** - Software defect.
16) **Philips BrightView, Cl II -** Software issues.
17) **Abbott m2000sp, Cl II** - some versions of Application Specifications (App Spec) are incompatible with m2000sp system software version 6.0 and 7.0. This may cause Error Code 9000 ("An unexpected error has occurred: Software error") to generated when screen is selected.
18) **Siemens Artis zee/zeego Angiography System, Cl II** - There is a potential issue on running Artis systems running software VC1x software if a network problem arises, the function cannot be deactivated again by pressing the "Block Radiation" key on the touch screen control. If this behavior occurs, the system image generation function is not available for patient examinations without switching the system off and back on again manually. This would result in no X-ray release and a delay in procedure.
19) **MEVION S250, Cl II** - Software defect that causes an incorrect dose compensation function to be applied to the internal dose ionization chamber when either pressure or temperature sensor malfunction. This could result in an incorrect dose delivery of no more than 5%.

20) **INOMAX DSIR Nitric Oxide delivery system, Cl II -** An issue has been identified in the INOmax DSIR system that could result in monitored Nitric Oxide (NO) concentration reporting lower than expected. This issue only pertains to those devices manufactured using a specific version of the Monitoring Circuit Board.
21) **VERO Linear Accelerator System, Cl II -** Software Anomaly; Because of a software bug, the VERO MHI-TM2000 Operator Console may provide Patient Positioning System (ExacTrac) with "Image Angle information used for the 1st port image", for a subsequent port image fusion. As the result, ExacTrac may display a Digitally Reconstructed Radiograph (DRR) image taken from the angle for the 1st port image fusion, rather than the one taken from the angle for the intended port.
22) **Q-Station Quantification Software, Cl II -** When using the QLAB Auto 2D Quantification (a2DQ) and Auto Cardiac Motion Quantification (aCMQ) applications, the reported End-Systolic Volume (ESV) may be smaller, and the Left Ventricular Ejection Fraction (EF) may be higher, than the ESV and EF calculated by manual tracing without the use of QLAB. An incorrect EF calculation could lead to misdiagnosis and/or delayed or incorrect therapy.
23) **QLAB Quantification Software, Cl II -** When using the QLAB Auto 2D Quantification (a2DQ) and Auto Cardiac Motion Quantification (aCMQ) applications, the reported End-Systolic Volume (ESV) may be smaller, and the Left Ventricular Ejection Fraction (EF) may be higher, than the ESV and EF calculated by manual tracing without the use of QLAB. An incorrect EF calculation could lead to misdiagnosis and/or delayed or incorrect therapy.
24) **Philips Brilliance iCT Computed Tomography, Cl II -** It was discovered that a software defect may result in the scanner not terminating the CT scan at the intended location.
25) **CARESTREAM DIRECTVIEW CR Software, Cl II** - Reduced mammographic image quality when attempting to print true size multi-format images.
26) **McKesson Cardiology ECG Management, Cl II** - Software error discovered in the McKesson Cardiology ECG Management with software versions 13.1 and 13.1.1.
27) **BrainLab iPlan RT Dose, Cl II** - iPlan RT Radiation Treatment Planning Software: Potentially incorrect patient positioning when using multiple localized CT image data sets.
28) **GE Revolution CT Cl II** - A required quality control test was not performed during installation associated with the software of the Revolution CT scanner.

There are other recalls where the software did play a passive part where it did not mitigate the problem where it was possible to mitigate it. If the companies would have done the risk analysis covering all bases, then they would have found the risks and mitigated them accordingly using, also, the software.

FCC Crackdown on Wi-Fi Blocking Applies to Hospitals

The AAMI writes that with the use of Wi-Fi hotspots on the rise, some commercial establishments have blocked wireless consumers from using their personal devices to access the Internet. A new enforcement advisory from the Federal Communications Commission (FCC) condemns the practice, threatens monetary penalties for violators—and has implications for healthcare facilities.

In its enforcement advisory, the FCC said "no hotel, convention center, or other commercial establishment or the network operator providing services at such establishments may intentionally block or disrupt personal Wi-Fi hotspots on such premises." Asked if the prohibition extends to healthcare facilities, a spokesman for the commission confirmed that was the case.

Apple iStore Update

Apple has amended its App Store Review Guidelines to forbid apps available through the firm's HealthKit framework from storing users' health data on the iCloud virtual server.

The policy (27.8) states: Apps that provide diagnoses, treatment advice, or control hardware designed to diagnose or treat medical conditions that do not provide written regulatory approval upon request will be rejected.

2015 Volkswagen Jetta Recalled To Fix Headlight Software Glitch

(Please note that this is not a medical device issue but a software recall issue.)

Volkswagen is recalling nearly 35,000 Jetta vehicles from the 2015 model-year to repair a problem with the cars' headlights. Unlike the headlight-related Acura recall issued yesterday, however, Volkswagen's recall stems from a software glitch.

FDA Cybersecurity Final Guidance

The final guidance released by the FDA, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," recommends that manufacturers consider cybersecurity risks as part of the design and development of a medical device, and submit documentation to the FDA about the risks identified and controls in place to mitigate those risks. The guidance also recommends that manufacturers submit their plans for providing patches and updates to operating systems and medical software.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

FDA Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices Guidance

The FDA has updated the MDDS guidance on 9 February 2015.

Even though you may decide to define some aspect of your system as a MDDS, it is still a medical device (class I) and needs to be validated and documented according to the FDA's guidance on software development.

http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm401996.pdf

FDA Mobile Medical Applications Guidance

The FDA has updated the Mobile Medical Apps guidance on 9 February 2015 to be consistent with the MDDS final guidance.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery

FDA Cybersecurity Webinar Report

Sherman Eagles of SoftwareCPR provides the following summary of some key points from FDAs webinar on their premarket cybersecurity guidance on October 29.

In the webinar, the FDA noted that the Instructions for Use should include what cybersecurity controls are needed in the use environment, but stated that it is not sufficient for a device to rely on a network being secure. The device manufacturer should identify the cybersecurity functions they have included in their device. Some of the core functions include:

- Limiting access to trusted users by using layered privileges, appropriate authenticity, and strong passwords.
- Protecting users and data by terminating sessions after a period of inactivity, setting up physical locks, and limiting access ports.
- Detecting, responding and recovering by implementing features that tell a user if the device has been compromised, provide information on what to do when it occurs, implement features to preserve critical functions with

the ability to reboot and recognize drivers, and provide methods for retention and recovery of device configuration.

They also expect to see a hazard analysis program that clearly evaluates risk potential, provides information on control put in place and the appropriateness of those controls to mitigate an identified risk, and a matrix that links cybersecurity controls to the risk being mitigated. Since the threat landscape will be continually evolving, they also want to see a plan for how the manufacturer will manage evolving threats. In response to a question, they indicated that updates for cybersecurity needed to manage new threats do not require a new premarket submission. Other questions brought out these points:

- Cybersecurity information is required for all submissions after October 1, 2014
- Risk to the system as a whole must be acceptable
- Mobile apps intended to control a device would need to consider cybersecurity
- Cybersecurity should be considered for any programmable logic
- There is no requirement for minimum strength of encryption, but they expect a rationale from the manufacturer for the encryption chosen
- A software device delivered from the cloud should consider environment and analyze it for cybersecurity risks
- Labeling could be used to mitigate cybersecurity risks if it clearly informs the user of the needed mitigations

All companies dealing with the Internet should note that this guidance is meant for them. We recommend that you review your cybersecurity needs and prepare a cybersecurity report for all submissions. As the FDA is learning the material in parallel to you, this will be a battle of who can convince whom first (you or the FDA) on whether you are meeting the cybersecurity requirements If you don't have a cybersecurity expert in-house, we can help support your needs with our experts.

FDA General Wellness: Policy for Low Risk Devices Guidance

The FDA has issued a draft guidance on low risk products intended for general wellness.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery

FDA Medical Device Accessories: Defining Accessories and Classification Pathway for New Accessory Types Guidance

The FDA has issued a draft guidance for medical device accessories to define accessories and classification pathways for new accessory types.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429672.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery

Distinguishing Medical Device Recalls from Medical Device Enhancements

The FDA issued a guidance entitled "Distinguishing Medical Device Recalls from Medical Device Enhancements" dated 15-Oct-2014. This guidance provides a series of examples as well as some explanation to help distinguish recalls, corrections, removals, and enhancements of medical devices. A number of the examples are for software changes. Some general principles relate to whether the change is being made because the device does not meet its specifications and claims and whether the device is violative (not in compliance with FDA law/regulation).

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM418469.pdf

FDA Draft Guidance Flow Cytometry Devices

The FDA issued a draft guidance entitled "Flow Cytometric Devices" dated 14-Oct-2014. Section 5 of this guidance addresses software used in the device and discusses regulatory clearance with the associated reagents and instrumentation as well as other information needed. The full guidance is at the link provided and was issued jointly by the Office of In Vitro Diagnostics Division of Immunology and Hematology and the Center for Biologics Evaluation and Research.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM418205.pdf

FDA IVD Device Level Of Concern

The FDA issued a guidance entitled Class II Special Controls Guideline: Nucleic Acid-Based In Vitro Diagnostic Devices for the Detection of Mycobacterium tuberculosis Complex and Genetic Mutations Associated with Mycobacterium tuberculosis Complex Antibiotic Resistance in Respiratory Specimens" dated 22-Oct-2014.

Section 5c of this guidance addresses software. In addition to referring to the general software guidance it specifically requests a clear description of how raw signals are converted into a result. It also has a lengthy discussion of level of concern. Although in section 4 it states the device can provide false negative results for tuberculosis allowing for disease progression and transmission to others. In Section 5c it stress Level of concern must be determined without considering mitigation and then says software would normally be considered moderate for this type of device but you must determine the actual level of concern from your hazard analysis.

Section 5c also states that "If any significant changes are made to the hardware or software after the completion of the clinical studies but before the clearance and distribution of the device, you must perform a risk assessment and include it in your 510(k) submission."

Section 5c then provides a list of references that may be helpful but note that the reference to AAMI SW68 is probably obsolete and was unintentional as the current medical device software lifecycle standard is EN/AAMI/IEC 62304.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM419468.pdf

Device Software Development Report

Seapine Software (seapine.com) which provides a variety of development tools published its 2014 report on the state of software development for medical devices. This report was generated based on input from 500 individuals in the medical device industry. It contains a breakdown of risk management methods used, key documentation challenges, requirements management approaches used, test management, traceability, and use of Agile methods. The report is at the link provided.

http://downloads.seapine.com/pub/papers/2014-state-medical-device-development-report.pdf

FDA Final Infusion Pump Guidance

The FDA issued a final guidance "Infusion Pumps Total Product Life Cycle" dated Dec. 2, 2014 after its draft of this document issued April 23, 2010. This supersedes the original "Guidance on the Content of Premarket Notification [510(k)] Submissions for External Infusion Pumps" issued March, 1993. This guidance mentions the word software 31 times and safety assurance case 15 times. It specifically states that the infusion pump system includes the network (i.e., any device or system physically or wirelessly connected to the infusion pump) and explicitly requests communications and network information in premarket submissions.

It also states that the following should be provided as part of the software design information: a drug library or other dose error reduction mechanism; a real time clock (RTC), On-board memory, Pump log Alarm handler; and Watch dog timer.

The guidance states 3 elements of safety cases: Claims, Arguments, Evidence and provides general guidance but states the format and methodology are flexible but should be well explained. It also states that FDA uses post market data in its review of safety cases to confirm their validity.

Section 5b lists 4 hazards to be addressed in the safety case: Delivery Error, Incorrect Therapy, Contamination, and Traumatic Injury. It goes on to list categories of hazards and specific causes to be considered.

In the software safety section of the guidance refers to the general FDA software submission guidance, the premarket cybersecurity guidance, and the one for Off-the-shelf software this guidance and then specifically requests static analysis of the software and extensive details required for each unresolved anomaly in terms of root cause analysis, analysis for similar bugs, and details on how to fix the anomalous code.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM209337.pdf

HHS to Investigate Medical Device Security

The U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) indicated that it would be investigating security of medical devices in hospitals during fiscal year (FY) 2015. The following statement is from the OIG FY 2015 work plan.

"We will examine whether CMS oversight of hospitals' security controls over networked medical devices is sufficient to effectively protect associated electronic protected health information (ePHI) and ensure beneficiary safety. Computerized medical devices, such as dialysis machines, radiology systems, and medication dispensing systems that are integrated with electronic medical records (EMRs) and the larger health network, pose a growing threat to the security and privacy of personal health information. Such medical devices use hardware, software, and networks to monitor a patient's medical status and transmit and receive related data using wired or wireless communications. To participate in Medicare, providers such as hospitals are required to secure medical records and patient information, including ePHI. (42 CFR � 482.24(b).) Medical device manufacturers provide Manufacturer Disclosure Statement for Medical Device Security (MDS2) forms to assist health care providers in assessing the vulnerability and risks associated with ePHI that is transmitted or maintained by a medical device. (OAS; W-00-15-42020; various reviews; expected issue date: FY 2015)".

FDA Final MDDS Guidance

FDA issued a final version of its guidance for "Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices". This guidance is very significant as it states FDA is exercising discretion and not requiring compliance to the recent regulation for MDDS and goes further to indicate this also applies to Medical Image Management Communication and Storage Devices.. The excerpt indicated this is repeated below and the full guidance is at the link provided.

"This means that for devices that meet the definitions in the regulations listed above, the FDA does not intend to enforce compliance with the regulatory controls, including registration and listing, premarket review, postmarket reporting, and quality system regulation for manufacturers of these types of devices."

https://docs.google.com/viewer?url=http%3A%2F%2Fwww.fda.gov%2Fdownloads%2Fmedicaldevices%2Fdeviceregulationandguidance%2Fguidancedocuments%2Fucm401996.pdf

IEC 62304 Update

The update for the IEC 62304 (Software Development Life Cycle) has passed and should be issued sometime in 2015. This update (listed as Edition 1.1) adds a flow for determining the Software Safety Classification, relates to validation of legacy software, and other miscellaneous clarifications and minor technical changes. A capability assessment for meeting the standard should be released as a separate Technical Report late 2014.

Edition 2 of the standard is in early draft stage in the committee and is expected to be released not before 2016.

Static Code Analysis

Static Code Analysis (SCA) is still a major issue and is being utilized by the FDA in more submissions than in the past.

SCA is an effective tool for cleaning up software bugs and enforcing your coding standard. Using a SCA on your code could free you from performing code reviews (if your SDLC Procedure covers it).

Accordingly, whether you are a high risk project (Major LOC, PMA, 510/K De Novo, infusion pump, or any other special case) or not, you should use the SCA during the development phase, with or without formal reports. Also, if you are a high risk project, we recommend that you use a FDA recognized SCA at around the code freeze to clean up the software and output a formal report to be sent to FDA as part of the submission.

We feel that in the future, the FDA will require the SCA report as a standard for all submissions (it saves them the trouble of asking for it and also asking for the source code).

Software V&V Process

There are many companies putting off the software V&V process. This is a mistake as you can't add quality to your software. The quality has to be built into the software from the requirements through the design. These companies think that they are saving money but, it is costing them money in the mid to long term. We highly recommend that companies start on the software V&V process early in the development and not later on.

There are also many companies maintaining the software documents as an afterthought after preparing the software documents properly. This afterthought is not in accordance with the regulatory requirements and makes the software maintenance process difficult to show.

We are still noticing Risk Analysis relating to software defects as a risk hazard cause. Potential software defects are not proper hazards as they do not yet exist. The only mitigation for this risk hazard would be to code review every line of source code.

Support Software Validation

According to the FDA and CE, all software used as a component, part, or accessory of a medical device, used in the production of a device, and used in implementation of the device manufacturer's quality system require validation. These software applications include ERP, CRM, QA, PLM, ALM, PDM, LIMS, HPLC, CAD and CAM applications as well as all software in production equipment.

You may ask if the scope of the validations are the same for all of the application types. The answer is that the scope of the validations may not be the same and there may even be major differences in their scopes of validation. This should be investigated.

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

Mike