SoftQuest Systems
assuring quality projects

June 30, 2021

Software in Medical Devices – Update for Q1/Q2 2021

The past year has been very difficult for all of us, from many different aspects. Not much has been happening in releasing new standards and the MDR has finally happened.

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

Software is everywhere in medical devices and IVDs. The FDA and CE are becoming more pedantic on how they review and relate to software. The number of companies getting into the field is growing and the amount of software being developed for medical is very large.

The is an emphasis on "digital health" where the FDA is fast-tracking many devices (even though it is only software, it is still a medical device). Just because it is software only, this doesn't mean that you are free from all the regulations, including a quality management system, risk analysis, etc.

There are rumors that the FDA will get rid of the differences in the documentation to submit for the Level Of Concern (LOC). If this happens, all submissions will probably be like a Major LOC of today, including the static code analysis report.

Software Recalls Q1-Q2 /2021

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. It is interesting to note that software is the leading cause of recalls in the FDA for the past 5 years. This trend does not look like it will change.

The following are additional examples of recalls involving software directly as listed on the FDA website. There were less recalls in this period relating to software than last year, but there were a number of class 1 recalls. There may be more but classified not under software. The descriptions given for the recall are taken from the FDA database. For further details on the recalls, you can check them out on the FDA's recall database.

POB 1124, Rehovot 7611101, Israel E-mail: mikez@softquest.co.il Web: www.softquest.co.il
Tel: 972-8-9493944 Mobile: 972-50-5357221 Fax: 972-8-9491681

- **Vero Biotech, GENOSYL DS, Class I** – Reports received of NO measured below desired dose during transition between primary console and backup console since Software Version 2.2.3 was uploaded to consoles in the field.
- **CareFusion, BD Alaris Infusion Pump Module, Class I** – Pump Module keypad lifting, and Fluid ingress could result in 1) Unresponsive keys: module continues infusion, PC unit will not alarm and must be used for programming changes, may necessitate a different Pump Module. May result in infusion start delay/inability to titrate medication. 2) Stuck keys: PC unit alarms, module exhibits Channel Error, may result in infusion interruption/start delay.
- **Vero Biotech, GENOSYL DS, Class I** – Reports received of NO measured below desired dose during transition between primary console and backup console since Software Version 2.2.3 was uploaded to consoles in the field.
- **Beckman Coulter, Access SARS CoV-2 lgG II Reagent, Class II** – SARS-CoV-2 lgG II numerical results may potentially be multiplied by a factor of 1000 on systems running with assay protocol file (APF) and access assay file (AAF) versions resulting in falsely elevated numerical values.
- **BIOCARE Medical, IntelliPath FLX, Automated Staining Instrument, Class II** – There is a potential that the automated staining instrument with software version 3.5.3.1 may move with random speeds in random direction across its range of motion. This could result in the instrument hitting end stops or running into other components on the working deck. This could also result in wash buffer being dispensed on random locations.
- **Siemens Medical Solutions, ACUSON Sequoia, Class II** – The ultrasound system averages the Mean Sac Diameter (MSD) and Gestational Sac Diameter (GSD) into the Estimated Date of Delivery (EDD) calculation. This may result in an incorrect EDD, which may influence patient management decisions regarding induction of labor and elective caesarean delivery, which may result in premature births.
- **Accuray Incorporated, TomoTherapy Treatment System, Class II** – "MLC tickle error" may result in the delivered dose to effectively rotate from the planned dose.
- **Abbott Laboratories, WorkMate Claris System, Class II** – Due to a software error, the user may lose functionality of the system or the screen may turn black during operation.
- **Fujifilm Medical Systems, Synapse PACS Software, Class II** – The software does not update measurements and calculations in the Clinical Reporting Application (CRA) when the ventricular trace is changed in the study by a different user.
- **GE Healthcare, Case Cardiac Assessment System for Exercise Testing and CardioSoft Diagnostic System Exercise Stress Testing ECG application, Class II** – If a certain sequence of events occur, the pdf test report that belongs to one

patient will appear in a different patient's record when viewed in an Electronic Medical Record (EMR) or a similar system.

- **Pear Therapeutics, reSET Mobile App, Class II** – Due to a software issue, patients with a urine drug screen (UDS) received access to a contingency management wheel spin for potential rewards regardless of the UDS results. Positive UDS results should not have resulted in access to a wheel spin.
- **Brainlab, ExacTrac Dynamic software, Class II** – Display of potential patient movement might be delayed to the user for high dose treatments.
- **Viewray, ViewRay MRIdian Linac System, Class II** – Software anomalies affecting the French, German and Italian versions of treatment delivery system (TDS) software.
- **Fujifilm Medical Systems, Synapse Cardiovascular, Class II** – Software versions 6.0.4 to 6.2.1 using Advanced Reporting -possibility that a previously assigned internal patient database ID can be reused for a new patient. It was discovered that this value does not increase when a patient merge activity is executed in a specific sequence.
- **CHANGE HEALTHCARE, Change Healthcare Enterprise Viewer, Class II** – A software defect was identified where the Image Styles defined by presentation states from CHRS are not displayed in CHEV.
- **Siemens Medical Solutions, Multitom RAX, Class II** – Siemens identified two issues, In some cases, it is possible to perform an image acquisition although more than 20% of the beam does not hit the detector. This may only occur when an organ program for the wall mode without top alignment is selected and the system is moved to the centered position. If afterwards the operator activates the top alignment, increases the collimation, and lifts the tube, the system allows examination even with the tube being misaligned to the detector position. Hence, it is possible to overshoot the detector by more than 20%. From a clinical point of view, it is highly unlikely for the operator to trigger the examination as the misalignment is visible due to the light field being out of range. AND In very rare cases it may occur that the calculated dose value exceeds the limit of 2 Gy. This may potentially occur only when an organ program for free exposure is selected, and the system uses incorrect (too small) source-to-image distance (SID) for calculating applied dose. Hence, the calculated dose is much higher than the actual applied dose causing the buzzer, which normally notifies the operator about the exceeded limit of 2 Gy, to get activated erroneously.
- **Medtronic Minimed, MiniMed 670G Insulin Pump, Class II** – Due to a software design issue, under certain conditions, a software fault is detected when a large bolus delivery at quick bolus speed completes. if the user is not aware of the amount of active insulin and delivers an additional bolus, there is a risk of insulin over delivery.

- **Draeger Medical, Evita V800, Class II** – Three separate and unrelated problems attributed to the software used in the Evita V600, Evita V800, Babylog VN600 and Babylog VN800: 1. Restart of ventilation unit. 2. Incorrect FiO2 high and FiO2 low alarms. 3. SmartCare/PS (SC/PS) suspends weaning.
- **Raysearch Laboratories, RayStation 4.5, 4.7, 4.9, 5, 6, 7, 8A, 8B, 9A, 9B, 10A, 10B, RayPlan 1, 2, 7, 8A, 8B, 9A, 10A, 10B, Class II** – For some LINAC types, merging clinical beams with beams of approximate dose may lead to the approximate dose erroneously labeled as clinical dose. Merge beams can be used manually, in scripting, or as part of the Automated breast planning feature. In some cases, when merging two beams where the first beam has clinical dose and the second beam has approximate dose, the dose of the resulting beam will be labeled as Clinical, although dose for some of the beam segments is still calculated with the SVD dose engine and it should be labeled Approximate: Mixed dose. The difference between approximate and final Clinical dose is in most cases small, but there can be body sites such as lung where the difference can be significant.
- **Haag-Streit, Eyesuite 9.3.1 software, Class II** – Examination data and patient name may be mixed up when printing or generating a pdf with the interface at Pacific Coast and Laser Institute (PCLI).
- **Medtronic, Percepta CRT-P MRI SureScan, Class II** – A longevity estimation error may occur in the early years of device life when a unipolar pacing vector is programmed in the right atrial (RA) lead and/or the right ventricular (RV) lead. No other device features or therapies are impacted.
- **Philips, Xper Flex Cardio, Class II** – Performance issues with the Xper Flex Cardio Physio Monitoring System include: potential delay of up to 10 seconds in displaying ECG, invasive blood pressure and other parameters; patient weight is rounded to the nearest whole kilogram;Xper IM software used with the Xper Flex Cardio Physio Monitoring System may periodically crash; No SpO2 numeric or plethysmography is displayed when SpO2 is connected to the Flex Cardio device; display of certain data from the FC2010 becomes frozen, i.e., waveforms cease sweeping and updating and the ECG, IBP, and respiration numeric values cease to update; ECG, IBP, and respiration waveforms become flat lines and no audible alarms are produced for HR and IBP, upon start up, an unexpected non physiological ECG waveform, erratic heart rate numeric value, and non-physiological display of any other active waveforms may appear on the Boom Monitor.
- **Change Healthcare, Change Healthcare Enterprise Viewer, Class II** – Change Healthcare has identified an intermittent software defect which may result in an anchor study failing to display.
- **Datascope, Cardiosave Hybrid IABP, Class III** – There are cybersecurity vulnerabilities in a widely used low-level TCP/IP software library that may

result in a loss of communication to the Hospital Information System/Clinical Information System (HIS/CIS).

- **Siemens Medical Solutions, Interventional Fluoroscopic X-Ray System, Class II** – Siemens has become aware of a potential issue with software version VE20C. Planned procedures may have to be terminated and performed on an alternative x-ray system.
- **Siemens Medical Solutions, Sensis/ Sensis Vibe Hemo systems with VD12A software, Class II** – Due to the configuration of certain Windows Service Permissions within the operating systems of the Sensis/ Sensis Vibe computer, there is a risk for exposure of sensitive information, manipulation of data, or Denial of Service attacks and could result in incorrect diagnostic or therapeutic decisions.
- **EOS Imaging, EOSedge system, Class II** – Inadequate images resizing and 2D measurement errors may occur when biplanar acquisition has been performed with patient orientation different from AP (Antero-Posterior).
- **Fujifilm Medical Systems, Synapse PACS, Class II** – The wrong patient information may be displayed in the viewer or PowerJacket.
- **Philips, SureSigns VM4, VM6 and VM8, Class II** – Fail to Comply with Chinese Standard YY1079-2008: Clauses 4.2.6 and 4.2.7.3. Range/accuracy of heart rate meter for pediatric mode-In pediatric mode, when the input signal rate is over 300 bpm, the indicated rate of the affected products will be lower than this upper limit.
- **Biomerieux, VITEK 2 Compact, Class II** – Biomerieux has identified a potential safety risk worst case of a false susceptible erroneous test result associated with this event. The problem is when HL7 Connection is used, the results in the VITEK¿ 2 do not match the results sent to the LIS and the Laboratory Technician would need to change results in the LIS to match those in the VITEK¿ 2. If the isolate is sent more than once to LIS, a software defect prevents the system from sending the expertised interpretation results and the Therapeutic Corrections (TC) is not sent to Laboratory Information Systems (LIS).
- **Raysearch Laboratories, RayCare 3B, Class II** – Patient related messages created in RayCare 3B, RayCare 4A will be lost when upgrading from RayCare 2 to RayCare 3B or later.
- **Hitachi Medical Systems, Arietta 850, Class II** – Arietta 850 software version 4.0.0., 4.0.1, and 4.0.2 has an error in the focus point and transducer aperture settings in the SWE function. When the affected software with SWE function is used in conjunction with the C252 probe, this error can result in out of specification MI/TI acoustic output. The MI/TI acoustic output is higher than regulatory limits.

- **Mindray, BeneVision Distributed Monitoring System, Class II** – BeneVision DMS may intermittently freeze and require a manual reboot after which normal operation resumes. If a freeze occurs, patients monitored on a telemetry transmitter will no longer communicate data to the BeneVision DMS.
- **Siemens Medical Solutions, CT VA30A_SP2, Class II** – SOMATOM systems-issues in with software syngo.CT VA30A_SP2 or syngo.CT VA30A_SP2a, may result in sporadic problems causing scanning workflow interruptions and unexpected user notifications. Delay in diagnosis or patient rescan may occur. Sporadic software errors during interventional workflows may also result.
- **Thermo Fisher Scientific, Cascadion SM Clinical Analyzer, Class II** – Due to software defect, under certain assay parameters, false Vitamin D results may be reported. The system reports a false result by not quantitating the correct analyte peak in sample chromatogram. The resulting sample would show a Vitamin D-concentration that is an unusual situation for human serum and plasma samples and would indicate a severe Vitamin D deficiency.
- **Canon Medical System, System INFX-8000C, Class II** – The x-ray irradiation field may shift with respect to image receiving surface displayed on the screen at some C-arm angles.
- **Brainlab, ExacTrac Dynamic, Class II** – In case of a failed automatic marker detection, a software error causes parts of the display to incorrectly behave as if the current patient position is within predefined tolerances and may allow the user to proceed to treatment despite potentially exceeding shift values.
- **Siemens Medical Solutions, Sensis / Sensis Vibe Systems, Class II** – System may sporadically freeze (lock-up) during operation or while being in an idle state, no longer possible to interact with the system.
- **Nihon Kohden, WMTS Telemetry Receiver, Class II** – Incorrect Date Stamp or No Data Transfer on Telemetry Receiver and Transmitter.
- **Siemens Medical Solutions, ARTIS Icono Biplane, Class II** – Misleading error messages and a gap in the Operator Manual which affects ARTIS Icono biplane or ARTIS Icono floor systems with software version VE20B. Potential issues include System error management, Erroneous error messages, Zoom/Pan Function, Grid Indication, and Coolant Level. May cause procedures to be terminated and performed on an alternative x-ray system.
- **Carl Zeiss Meditec, IOLMaster 700, Class II** – When using software 1.90.2.09 or 1.90.8.06 and using modality worklist functionality for patient data transfer, the selection of the patient in the patient list may not match the patient information displayed on the right side of the screen.
- **Draegar Medical Systems, Infinity Acute Care System (IACS) Monitoring Solution, Class II** – The Infinity M540 patient monitor may randomly reboot

due to an error to correctly transmit and read the header data of files in the memory of the device. Under this situation, the device will try to reboot to mitigate the error. The device will be available again for use within 30 seconds. If this error continues and the M540 reboots three times in a time span of 10 minutes, it will enter a fail-state. A fail-state will annunciate itself with a continuous sound to alert the user. The M540 will reset to factory default and the user can manually configure and readmit the patient to continue patient monitoring.

- **Roche Diagnostics, 9180 Electrolyte Analyzer, Class II** – May display Calcium results on the screen with wrong arrow direction which may lead to misinterpretation of results and incorrect medical decision. If the unit for iCa++ is set to mg/dL (configured as Service Code MGL) and a measured iCa++ value is lower than the normal range, an upward arrow is shown on the display instead of a downward arrow. The display is set per default to mmol/L; therefore, the arrow indicating an alarm reflects normal ranges of iCa++ in mmol/L. If mg/dL is chosen, the arrow warnings on screen still reflect the ranges from mmol/L, rather than mg/dL. The numeric result is displayed correctly.
- **Topcon Medical Systems, Harmony Referral System, Class II** – Harmony RS integrations with Topcon equipment, TRC NW-400 and the Signal Camera, allowed user input of non-unique patient IDs that caused multiple patient records and images to be combined under the first generated record.
- **Biomeme, Franklin Real-Time PCR, Class III** – Users cannot complete testing due to a sign-error in the software component that controls the filter movement and results in an instrument failure and assay failure before results are generated.
- **Baxter Healthcare, Flow Coupler Monitor, Class II** – Potential for the battery to lose its ability to be recharged.
- **Roche Diagnostics, Calculator/data processing module, Class II** – A software error results in the unintentional removal of the serum-indices flag that would otherwise prevent the release of results. The Cobas Inifinity has an auto-verification feature to hold results for manual review when they meet specific criteria. The serum indices flag is used for serum indices tests that are performed to assess the quality of the sample (e.g., hemolysis, icterus, and lipemia). Normally, when the Cobas Infinity receives a result for a test that is serum indices-sensitive, it flags the result, and the software then waits for the results of the serum indices tests before validating or rejecting the test result. Roche has discovered a software error that under specific conditions causes the flag to be incorrectly removed. This allows for the possibility that a sample of poor quality may return an unreliable/incorrect test result that is mistakenly reported to the health care provider and/or patient without the proper disclaimer that the result is based on a sample of poor quality.

- **Roche Molecular Systems, uPath software, Class II** – When a user creates a measurement tool annotation in the uPath Enterprise software version 1.1, the measurement value is incorrectly calculated when the measurement is viewed in "Split View" viewing mode and the slides within the case are scanned at different magnifications.
- **Philips Ultrasound, EPIQ and Affiniti Ultrasound systems, Class II** – The manufacturer has determined that with certain uncommon workflows there is potential for incorrect patient data to be displayed and saved into an exam. The issue(s) manifest differently for different versions of software.
- **ICU Medical, ICUmedical Cogent Hemodynamic Monitoring System, Class II** – Due to a potential software issue, the display may show the incorrect continuous cardiac output (CCO) values after PulseCO calibration.
- **Siemens Medical Solutions, Artis Zee/ Zeego & Artis Q/ Q.zen, Class II** – When the user changes frame rates from lower frequency (e.g. 10 f/s) to higher frequency (e.g. 30 f/s) during continuous release of Fluoro "Fluoro Override", the measured Air Kerma Rate can exceed the regulatory limits.
- **Ortho-Clinical Diagnostics, VITROS Automation Solutions, Class II** – A software anomaly may cause an aliquoted sample to be labelled as the incorrect sample. This may lead to results being associated with the wrong patient sample and potentially lead to inappropriate intervention with the potential for injury to the patient.
- **Siemens Medical Solutions, SOMATOM Force, Class II** – System does not trigger a cancel command followed by a reload of the scan with the new parameter(s). This issue may result in a delay in diagnosis and/or need for patient rescan.
- **Medtronic Neuromodulation, Intellis Spinal Cord Stimulator, Class II** – A710 Intellis Clinician Application has a software issue that can result in the inability to program the Intellis implantable neurostimulation device.
- **NeuMoDx Molecular, NeuMoDx Cartridge, Class II** – There is a potential for false positive results when certain lots of cartridges are used in conjunction with specific assays.
- **GE Healthcare, Revolution EVO, Optima CT660, Optima CT680 CT Systems, Class II** – Improperly loaded software options may result in additional X -ray radiation exposure to the patient.
- **GE Healthcare, CASE and CardioSoft, Class II** – If a certain sequence of events occurs, the pdf test report that belongs to one patient will appear in a different patient's record when viewed in an Electronic Medical Record (EMR) or a similar system.
- **Pear Therapeutics, reSET Mobile App, Class II** – Due to a software issue, patients with a urine drug screen (UDS) received access to a contingency

management wheel spin for potential rewards regardless of the UDS results. Positive UDS results should not have resulted in access to a wheel spin.

- **GE Healthcare, Innova IGS 3, Class II** – The IGS system can experience a single vertical line defect where the vertical line divides and horizontally shifts live monitor images into two unequal image parts within the monitor display screen.

IEC 62304 Update

As of 01 May 2021, the IEC 62304 draft that is in the works has been rejected. The project is closed. This means that IEC 62304:2006 + Amd1:2015 will remain valid for some more years to come.

Whether this is good or bad, all depends on how you see the IEC 62304:2006 + Amd1:2015 standard. There are items I would like to have more clarified and other items handled differently than they are handled today. Overall, it is not a bad standard and it's here to stay in its current form for the next few years.

MDR and IVDR

MDR is in effect, including software. In Europe MDSW (medical device software) is defined as:

"Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."

Software serving a medical purpose is considered a medical device and, shall comply with the EU Regulation 2017/745 (MDR) or EU Regulation 2017/746 (IVDR).

MDR Article 2 specifies that stand-alone software is considered a medical device if it is intended to be used by the manufacturer for one of the following purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state

- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations

IVDR Article 2 defines that software is an IVD if it is used to provide information on one or more of the following:

- concerning a physiological or pathological process or state
- concerning congenital physical or mental impairments
- concerning the predisposition to a medical condition or a disease
- to determine the safety and compatibility with potential recipients
- to predict treatment response or reactions
- to define or monitoring therapeutic measures

Medical Device Cybersecurity

Cybersecurity has been an area of growing concern for FDA. In response, CDRH has created a device cybersecurity division. Recently, the agency announced that it had appointed Kevin Fu as acting director of this new division. Fu is a prominent medical device security researcher at the University of Michigan and the founder of its Archimedes Center for Medical Device Security. He has been very active in training medical device company personnel in cybersecurity engineering. Although it is only a one-year appointment and Fu will return to his role at the University of Michigan thereafter, his appointment is being hailed as a signal that FDA has elevated its treatment of cybersecurity. Fu has told medical device manufacturers that they will see a new FDA cybersecurity draft guidance this year.

Cybersecurity breach in Las Vegas Hospital

A cybersecurity breach at a Las Vegas hospital has led to the personal information of patients' being exposed online. The hackers gained access in mid-June to a hospital server with the data. While there is no evidence that any clinical systems were accessed, patients and employees were notified that their personal information may be at risk.

Artificial Intelligence/Machine Learning-Based Medical Software and Digital Health

In January 2021, FDA issued its Action Plan for Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD), building on its April 2019 Proposed Regulatory Framework for Modifications to AI/ML-Based SaMD. Although it is not a formal guidance, the action plan does summarize FDA's current thinking on the subject and is intended to further discussion on this topic and elicit comments and feedback that FDA may use to formulate guidance planned for later this year. Significantly, the action plan indicates that because AI/ML-based SaMD continuously learns and modifies its algorithms, it would be impractical to solely regulate the technology under FDA's regulatory framework for SaMD. Thus, FDA is thinking that pre-market submissions for AI/ML-based SaMD can be used by the agency to review and assess the range of modifications to devices that can be expected to result from the AI/ML and how such modifications would both stay within that range and occur in a controlled manner.

In the digital health field, FDA is expected to continue its efforts to improve the review and availability of digital health medical products, including better coordination between FDA's drug and device centers. FDA's Digital Health Center of Excellence will lead these efforts. Note that some members of Congress have been critical or skeptical of FDA's digital health plans. These members include Senator Patty Murray, who now leads the Senate Committee on Health, Labor and Pensions and can be expected to increase Congressional scrutiny.

CDER Guidance Agenda New & Revised Draft Guidance Documents Planned for Publication in Calendar Year 20211 (January 2021)

- Use of Digital Health Technologies for Remote Data Acquisition in Clinical Investigations
- Regulatory Considerations and Drug Labeling Recommendations for Prescription Drug Use-Related Software for Combination Products
- Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers

FDA release 12/1/21 Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan

The AI/ML-Based Software as a Medical Device Action Plan outlines five actions that the FDA intends to take, including:

- Further developing the proposed regulatory framework, including through issuance of draft guidance on a predetermined change control plan (for software's learning over time);
- Supporting the development of good machine learning practices to evaluate and improve machine learning algorithms;
- Fostering a patient-centered approach, including device transparency to users;
- Developing methods to evaluate and improve machine learning algorithms; and
- Advancing real-world performance monitoring pilots.

FDA Guidance on QMS Validation: 4 Major Changes

1) **Increased focus on computer system validation**
   Computer system validation (CSV) is the process of achieving and maintaining compliance with relevant GxP regulations defined by the predicate rule.

2) **Increased focus on critical thinking and software assurance**

   To this end, you can begin applying critical thinking by using a risk-based approach to assess the system's features, focusing on the direct impact to patient safety and device quality. By applying this risk-based methodology, you will need to assess what happens in the event there is a system failure.

3) **Increased focus on the supplier management relationship**

   Given that you will be relying on the supplier's quality system to support your software's compliance activities, more scrutiny on vendor quality assurance is almost guaranteed.

   As such, effective quality assurance and management should incorporate a collaborative combination of process and product audits.

   The sooner you identify and correct supplier quality issues and non-conformances, the sooner you'll be able to activate on corrective policies and procedures.

4) **Recognize computer system validation isn't a paper exercise**

   Old-school validation requires mountains of documentation to assure the system's suitability for the intended use. That being the case, it may take a

shift in your quality assurance team's thinking here to understand the change in approach.

Unfortunately, just executing test scripts may not uncover system issues. For the best results, users must "play" inside the system. This unscripted test approach is much better in uncovering bugs, quirks, or failures inside the system.

Computer Software Assurance (CSA) vs. Computer Software Validation (CSV): FDA Adopts a Risk-Based Approach for Software Validation

The FDA is expected to release a new guidance document, Computer Software Assurance for Manufacturing, Operations and Quality System Software, in 2021.

FDA says goodbye PACS, hello MIMPS

The FDA on 19/4/21 has changed its regulatory classification of PACS (Picture Archiving and Communication Systems), referring to it now as MIMPS (medical image management and processing systems) as part of amended regulatory classification changes made for radiology-specific software.

Whether or not this will have an effect on the submissions is open for discussion.

FDA Recognized Consensus Standards (since last update)

- IEEE Std 11073-40101-2020, Health informatics - Device interoperability Part 40101: Foundational - Cybersecurity - Processes for vulnerability assessment.
- IEEE Std 11073-40102:2020, Health informatics - Device interoperability. Part 40102: Foundational - Cybersecurity - Capabilities for mitigation.
- ANSI ISA 62443-4-1-2018, Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements.
- CVSS v3.0, Common Vulnerability Scoring System version 3.0

New FDA Standards (since last update)

- Safer Technologies Program for Medical Devices - Guidance for Industry and Food and Drug Administration Staff

Previously listed: FDA's Software Related Prioritized Medical Device Guidance Documents to Publish in FY 2021

A-List Final Guidance Topics:

- Safer Technologies Program for Medical Devices **– released (see above)**
- Clinical Decision Support Software **– in process**
- Device-Specific Criteria Guidance(s) for Safety and Performance Based Pathway Implementation **– in process**

A-List Draft Guidance Topics:

- Content of Premarket Submissions for Software Contained in Medical Devices **– in process**
- Content of Premarket Submissions for Cybersecurity of Medical Devices **– in process**
- Computer Software Assurance for Manufacturing, Operations, and Quality System Software **– in process**

B-List Draft Guidance Topics:

- Risk Categorization for Software as a Medical Device: FDA Interpretation, Policy and Considerations **– in process**

FDA's Cybersecurity Guidance Update

So far this year, the FDA has not released a new draft guidance for cybersecurity.

When and How to Use Sub-contractors for Software Development

There are pluses and minuses in using sub-contractors to develop the software of a medical device. If the company is a start-up, it usually doesn't have the resources to develop quality software. In this case, the decision to use a sub-contractor comes easy. It makes sense to use a good sub-contractor to develop

the software. The question arises, what to allow the sub-contractor to do and how to control the work being done.

When discussing the project with the sub-contractor, he will swear that he knows what the regulatory bodies want, he knows the standards, he knows how to develop the code according to required guidelines, he knows how to write the documents, he knows how to validate the software, etc.

It's very probable that the sub-contractor has worked on a number of projects that have cleared the FDA/CE. The clearance can be due to good software documentation produced or due to more luck than experience, as the reviewer did not review the documentation in depth.

Additionally, the sub-contractor will tell you he can write the software requirements and validate them. Would you let the cat watch the cream? As you know what is required, you should write the software requirements specifications. If the sub-contractor writes the software requirements, they will reflect what the software actually does and not what you required.

Accordingly, you should also validate the software according to the requirements. You know what is expected and this way, you can make sure the software meets the formal requirements defined.

You should also have a SOW (Statement of Work) with the sub-contractor detailing the scope of work, documentation standards, participation in audits (internal, external) if required, implementation documentation (unit test summaries, integration test summaries, code review summaries, verification testing summaries, etc.) on your forms (not the sub-contractor's forms), etc.

The sub-contractor should be trained according to your SDLC procedure (even if they tell you that they are certified). You do not want your external auditor (FDA/NB) deciding that they want to audit your sub-contractor.

Sub-contractors developing software (firmware, mobile, cloud, AI, etc.) who are looking to expand their portfolio and get deeper into medical devices are invited to contact me to find out what is required from them and how they can get their message to the companies looking for software development.

Software Safety Classes (IEC 62304) versus Levels of Concern (FDA)

Both, IEC 62304 and the FDA (Content of Premarket Submissions for Software Contained in Medical Devices) distinguish three different categories of medical

device software. The IEC 62304 uses the software safety classes (SSC) and the FDA guideline uses the Level of Concern (LOC). This causes much confusion.

The SSC is defined as follows in IEC 62304:2006 + A1:2015:

- The software system is software safety class A if:
  - The software system cannot contribute to a hazardous situation; or
  - the software system can contribute to a hazardous situation which does not result in unacceptable risk after consideration of risk control measures external to the software system.
- The software system is software safety class B if:
  - The software system can contribute to a hazardous situation which results in unacceptable risk after consideration of risk control measures external to the software system and the resulting possible harm is non-serious injury.
- The software system is software safety class C if:
  - The software system can contribute to a hazardous situation which results in unacceptable risk after consideration of risk control measures external to the software system and the resulting possible harm is death or serious injury.

The LOC is determined as follows in the FDA's Content of Premarket Submissions for Software Contained in Medical Devices:

- Major: We believe the level of concern is Major if a failure or latent flaw could directly result in death or serious injury to the patient or operator. The level of concern is also Major if a failure or latent flaw could indirectly result in death or serious injury of the patient or operator through incorrect or delayed information or through the action of a care provider.
- Moderate: We believe the level of concern is Moderate if a failure or latent design flaw could directly result in minor injury to the patient or operator. The level of concern is also Moderate if a failure or latent flaw could indirectly result in minor injury to the patient or operator through incorrect or delayed information or through the action of a care provider.
- Minor: We believe the level of concern is Minor if failures or latent design flaws are unlikely to cause any injury to the patient or operator.

The SSC classes determine the software life-cycle development processes to be performed and documented. Class A has the least processes and documentation

required and Class C has the most. The SSC is determined at the beginning in the project.

The LOC determines the document to be submitted as part of the submission (and not as part of the development process). The LOC must be determined before the submission. It has been known in numerous cases, that the FDA has determined the LOC is different than what the company determined (the FDA always wins).

There is a virtual connection between the SSC and the LOC, but they both relate to different aspects (processes and documentation vs. documentation to be submitted) and should be handled accordingly.

FDA Responses to 510K Submissions - Software

We are still receiving responses from the FDA concerning their software. This means that this is becoming the state of the practice for the FDA. These responses relate to the run-time testing, and cybersecurity. Below is shown the wording received from the FDA in all the cases:

1. 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
2. The information security and cybersecurity of the device is needed to evaluate the cybersecurity risks and the associated controls. The FDA has been asking for the cybersecurity even from devices that have no connectivity.

   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.
3. The FDA has been reading the software documentation, including the Risk Analysis, SRS, SDD, STD, STR, Traceability Report, OTS Report, Cybersecurity, etc. They have been raising issues as shown in the following:
   a. SRS: contradictions and not containing information necessary to understand the requirements for your device software; requirements related to programming language requirements or to the interfaces.
   b. SDD: high-level architecture and does not include the level of detail expected for software architecture; does not include information necessary to ensure that your software is safe and effective for the intended use of the device; missing information for all the third-party devices used by your system.
   c. Traceability Report: traceability documentation does not link between requirements to the hazards
   d. Testing: it doesn't include a summary of the static analysis, examples of unit integration testing, and a summary of the results.

We are highly recommending to clients several remediations:

1) SSC Class B/Moderate LOC - software 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++, Java, C#/VB.NET), Microsoft Visual Studio Static Code Analysis (C/C++), IAR C-STAT static analysis (C/C++), etc.
2) SSC Class C/Major LOC/Special Guidance/PMA – FDA will ask for a SCA report. We highly recommend using one of the tools that we know the FDA has evaluated. A partial list of these tools is Parasoft, Coverity, Polyspace, PQRA, Klocwork, Grammatech and LDRA.
3) A cybersecurity report should be prepared for submission to the FDA based upon the threat analysis.

4) Using tools for cybersecurity testing, penetration testing, etc.

When choosing SCA and cybersecurity tools, check the local support. Even though everyone offers Internet support, nothing beats having the support done locally by someone who has the experience and speaks your language.

Summary

There are many ways to screw up your software in the medical device whether it is embedded in dedicated hardware (also known as SiMD – Software in a Medical Device) or stand-alone health software (also known as SaMD – Software as a Medical Device). It doesn't take too much talent to do this (as we all know) and companies are doing it daily. Many companies mess up royally and don't know how to get out of the mess. In many cases, they don't even know that they are in deep trouble until the recall is issued.

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

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

Mike

POB 1124, Rehovot 7611101, Israel E-mail: mikez@softquest.co.il Web: www.softquest.co.il
Tel: 972-8-9493944 Mobile: 972-50-5357221 Fax: 972-8-9491681