

December 31, 2019

Software in Medical Devices – Update for Q3/Q4 2019

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.

There 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 Q3-Q4 /2019

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 4 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 about 250 recalls in this period relating to software, including numerous (greater than 10) 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.

- 1) **Quantum Pump Console, Class I** – Potential for Quantum Pump Console, part of the Quantum Perfusion Systems, to unexpectedly shut down while in use.
- 2) **HAMILTON-G5, with software versions less than or equal to 2.60, Class I** – New software version for affected ventilators reduces the probability of the

ventilator entering an ambient state, in which the inspiratory channel and expiratory valves are opened, letting the patient breathe room air unassisted. When the ventilator enters the ambient state, alternative ventilation must be provided immediately.

- 3) **Rosa Brain 3.0, Class I** – The instrument holder may be sent on a trajectory that is not within the intended target. If it is not corrected, the associated device may be placed incorrectly.
- 4) **Medfusion Syringe Pump, Model 4000, Class I** – There is an anomaly in Medfusion 4000 Syringe Pump Firmware version 1.7.0 that could potentially result in loss of primary audible and visual battery alarm functionality, and interruption of therapy.
- 5) **Minimed Model 500 Remote Control for use with the MiniMed 508 Insulin Pump, Class I** – There is a potential security vulnerability related to the use of the remote controller accessories with the insulin pumps.
- 6) **VOLUMAT MC AGILIA US, Infusion Pump, Class I** – The firm is correcting four software anomalies and KVO (keep vein open) end of infusion alarm priority in Software versions 1.7 and 1.9a of Volumat MC Agilia Software and versions 1.0 and 1.1 of Vigilant DrugLib.
- 7) **Vigilant Agilia, Vigilant DrugLib, Class I** – The firm is correcting four software anomalies and KVO (keep vein open) end of infusion alarm priority in Software versions 1.7 and 1.9a of Volumat MC Agilia Software and versions 1.0 and 1.1 of Vigilant DrugLib.
- 8) **Neuro Omega System, incorporating HaGuide software, Class I** – If cables are improperly connected, current may reach high charge density, causing tissue harm.
- 9) **Spine & Trauma 3D Navigation 1.0, Class I** – In certain occurrences, the affected navigation software application might unexpectedly display a navigated instrument in an axial, coronal/sagittal (ACS) view representation with fixed planes in the image reconstruction (the not-updated ACS view), instead of displaying the desirable view representation Inline View , which is commonly used for navigating invasive instruments at the spine. This could lead the surgeon to be unable to determine the position of the navigated instrument. This might occur after a crash restore or after changing between different navigation workflows during the same patient treatment.
- 10) **LIFEPAK 15 Monitor/Defibrillator, Class I** – Certain LIFEPAK 15 Monitors/Defibrillators were reported to experience a lockup condition after a shock was delivered. This condition is defined as a blank monitor display with LED lights on, indicating power on the device, but no response in keypad and device functions.
- 11) **Sphera DR MRI SureScan, Dual chamber rate responsive pacemaker (DDDR), Class I** – A subset of Medtronic dual chamber pacemakers distributed worldwide between 10 March 2017 and 7 January 2019 under

the brand names Adapta, Versa, and Sensia when programmed to a dual chamber mode with atrial-sensing, may experience a circuit error that affects device functionality.

- 12) **VNS Therapy, SenTiva, Class I** – Certain Model 1000 generators (SN = 100,000) have experienced unexpected device resets, which resulted in disablement of therapy. Fourteen (14) complaints have been reported. Each of the device resets occurred within 30 days of enabling therapy. Once the device is disabled, therapy can be re-enabled, but the device will continue to be susceptible to resets. If a device experiences this issue and is disabled, patients may return to baseline seizure or depressive symptoms.
- 13) **RayStation stand-alone software treatment planning system, Class II** – Editing a static arc beam may unexpectedly set the MU of the beam to its initial default value of 200 MU. If the bug is triggered, the dose is invalidated and needs to be recalculated before the plan can be approved or exported.
- 14) **CARESCAPE Central Station/CIC Pro Clinical Information Center Central Station/ApexPro Telemetry System, Class II** – When connected to the Mission Critical (MC) and /or Information Exchange (IX) networks, certain versions of the CARESCAPE Telemetry Server, ApexPro Telemetry Server, CARESCAPE Central Station (CSCS) version 1 and Central Information Center (CIC) systems were identified to have vulnerabilities to a cyber-attack.
- 15) **OARtrac Plus Clinical Detector Unit, Class II** – May result in readings outside of the expected accuracy range.
- 16) **MICRO-PSD External Beam Photon/MICRO-PSD HDR, Class II** – May result in readings outside of the expected accuracy range.
- 17) **Aestiva MRI, Class II** – Certain Aespire and Aestiva Anesthesia Systems were noted to have a vulnerability to a cyber-attack when connected to the hospital network. An insufficiently secured terminal server may provide an opportunity for a malicious actor that has already penetrated the hospital network to send fraudulent flow sensor correction parameters.
- 18) **Artis zee/ zeego Interventional Fluoroscopic X-Ray System, Class II** – In affected Artis zee floor Interventional Fluoroscopic X-Ray Systems, the activation of a collision sensor will cause a block the movement of the floating tabletop and could result in a delay or interruption of a procedure.
- 19) **Monaco Radiation Treatment Planning System (RTP) System, Class II** – Monaco is using the incorrect energy when optimizing and calculating dose.
- 20) **Alintiy S System, Class II** – Two software issues have been identified for the Alinity S System containing software version 2.0.0: Alinity's Probe Wash: When Alinity's CMV IgG Qualitative assay is run as the last assay on a sample, one of two unexpected events may occur: - An insufficient wash of the probe. The insufficient wash may compromise the following sample aspirated with that probe, potentially causing a false reactive result for any of the assays run. All other assays, when run in any position in a profile, have

sufficient probe washes -The embedded software may shut down unexpectedly. This shutdown may be recovered in less than 8 hours. The operations manual provides instructions in the event of an unexpected shutdown.

- 21) **iGUIDE System with software build iGuide 2.2.0, 2.2.1, and 2.2.2, Class II** – Potential for iGUIDE to incorrectly monitor the 3D position. Sometimes, although the HexaPOD has reached the target position, the Constant Correlation Check (CCC) can be too sensitive and iGUIDE may incorrectly demand a verification scan.
- 22) **Merge PACS versions 7.3, 7.3.1, 8.0 and 8.0.1, Class II** – Potential for prior thumbnails to not display in reverse chronological order and images may not scroll in reverse chronological order when mammography stacked scrolling is enabled. Merge PACS provides image manipulation tools to enable users to view and compare images such as: linking, MPR, MIP, 3D image fusion/registration of CT, MR and PET; as well as CVR (Color Volume Rendering), measurements (linear distances, angles, areas, SUV, etc.), and annotations (for example, outline and label regions of interest, label spinal vertebrae).
- 23) **Merge OrthoPACS versions 7.3, 7.3.1, 8.0 and 8.0.1, Class II** – Potential for prior thumbnails to not display in reverse chronological order and images may not scroll in reverse chronological order when mammography stacked scrolling is enabled. Merge PACS provides image manipulation tools to enable users to view and compare images such as: linking, MPR, MIP, 3D image fusion/registration of CT, MR and PET; as well as CVR (Color Volume Rendering), measurements (linear distances, angles, areas, SUV, etc.), and annotations (for example, outline and label regions of interest, label spinal vertebrae).
- 24) **C3 Wave App, v. 2.0.5, Class II** – When the iPad is updated with Apple iOS software version 12, the C3 application malfunctions. Upon launching a new procedure, the ECG waves do not appear on the screen, in surface or internal mode. If the C3 application is not operating properly, the PICC procedure must be completed without using alternate methods to confirm PICC tip placement.
- 25) **OptiLITE IX Laser Surgery Accessories, Class III** – It has been determined that a lot of fiber lasers were programmed incorrectly. As a result, the fibers from this lot will produce an error and will not allow the user to use the laser when it is plugged in.
- 26) **V-Twin, Model # 6002-800, UDI: 03661540600180, Class II** – Instrument stopped working due to a software lockup, and no patient results are produced.
- 27) **HS HiR NEO 900A NIR, Class II** – Software error in the central control unit of the floor stand.

- 28) **HS Hi-R NEO 900, Class II** – The Error only occurs in combination with the following floor stands FS 2-21, FS 2-25, FS 3-45 with the software REF 615 586 in the versions 10.1.xx to 11.3.xx
- 29) **Kaluza C Flow Cytometry Software, Class II** – Compatibility issue between the software and Microsoft updates to Windows 7, 8, and 10. The compatibility issue causes the software to be unusable which could result in a delay of reporting results.
- 30) **Recall EndoTool SubQ, Class II** – Product was distributed prior to approval or clearance from FDA.
- 31) **Dario Blood Glucose Monitoring System, Class II** – The Dario-Blood Glucose Tracker Android App versions 4.3.0-4.3.2 may experience duplicate logging of a blood glucose level reading.
- 32) **FastA1C Test AtHome A1C System/Walgreens At Home A1C Test Kit/A1CNow SELF CHECK/A1CNow+ Systems (professional use product)/CVS Health At Home A1C Test Kit, Class II** – A numerical value less than 4% or greater than 13% may be displayed instead of the expected <4% or >13% result, due to a software bug.
- 33) **VisuMax Femtosecond Laser, Class II** – VisuMax devices with software version 2.10.13 and activated SW-Module ReLEx (SMILE) option may experience a software issue. In case of a suction loss during treatment the software allows the user to choose the option immediate restart or restart treatment. Suction loss can occur in phase 1 through phase 5. The software defect refers to Phase 2 (between 10% and 100% of lower lenticule cut) only. The software offers a flap cut, but due to the software issue it performs a cap cut instead of a flap cut if the user proceeds.
- 34) **VNS Therapy Program, Class II** – A This recall is being initiated due to reports that that the therapy programming tablet with software version 1.5 errantly performs a normal mode diagnostic test instead of the selected system diagnostic test on Model 102 and Model 102R devices, if the output current is greater than 0.5mA. This can result in false high impedance values during patient follow-up.
- 35) **Atellica CH 930 Analyzer, Class II** – Potential for calibration error resulting in QC failures after the calibration run with QC and patient results being 5 times higher.
- 36) **SOMATOM go.Top, Class II** – SOMATOM go.Top (Models #11061640 & 11061648) with software syngo CT VA20A_SP2 and active Guide&GO license No dose documentation and no Dose Alert for the special mode i- Sequence during interventional procedures.
- 37) **Infinity M300, Class II** – The devices have potential cybersecurity vulnerabilities, which can include Distributed Denial of Service (DDoS), Spoofing, and Tampering.

- 38) **Syngo CT VB20, Class II** – Software issue identified in the software versions syngo CT VB20 running on the SOMATOM CT Scanner: scan aborts and system crashes.
- 39) **Omnipod DASH Insulin Management System, Class II** – There is a potential for a communication interruption following a bolus command that may result in inaccurate information presented in insulin on board (IOB), last bolus field or bolus history.
- 40) **LivaNova VNS Therapy System, Class II** – Lead impedance values reported by the affected VNS generator will be higher compared to those reported by previous models. This is due to a change in the timing of when affected VNS generator takes the lead impedance measurement during diagnostic testing. As a result, normal impedance ranges for the affected VNS generator have shifted relative to the existing thresholds of 600 - 5300 Ohms defined in labeling and as present in the programming software.
- 41) **Prismaflex Control Unit, Class II** – Communication error alarms may result in interruption of therapy, delay in therapy, or blood loss due to non-restitution of blood in the extracorporeal circuit.
- 42) **Infinity Acute Care System (IACS) Monitoring Solution with the Standalone Infinity M540 patient monitor, Class II** – Cybersecurity vulnerabilities may cause device to reboot, lose alarm functionality, and/or lose communication with cockpit and/or the Infinity Network.
- 43) **ApexPro Telemetry Server System, Class II** – May not provide visual and/or audible alarms at the CARESCAPE Central Station or Clinical Information Center monitor for ECG arrhythmias, ECG LEADS FAIL or Pulse Oximetry (SpO2) under certain conditions.
- 44) **Torrent Suite Dx Software Version (IUO) 5.4, Class II** – Torrent Suite™ Dx analysis software, a component of the Ion PGM Dx Instrument System, incorrectly displays a positive result when a different analytical or de novo variant is detected at the same locus as a specified clinical variant.
- 45) **Mammomat Revelation with software version VC10 and Biopsy Option, Class II** – An error can occur when performing a biopsy using the InSpect function. The acquisition workstation may become unresponsive to normal user interaction, can only take place in rare cases.
- 46) **Siemens Atellica CH 930 Analyzer, Class II** – Erroneous Indices for Hemolysis and Lipemia in Software versions 1.19.2 and below.
- 47) **Viva-ProE Systems, Class III** – Software malfunction; The action being taken due to the device becoming inoperable due to software lockup.
- 48) **Monaco RTP System, Class II** – It is possible that the forced electron density settings will be changed for some structures unintentionally and this can result in incorrect dose calculation.
- 49) **Dynex DSX Software-IVD ELISA Assays, Class II** – Assay files used on the open Dynex DSX Instrument to process IVD ELISA samples-programming

error results in well H6 being skipped for the addition of the TMB substrate. Well H6 will generate a negative result regardless of whether the patient was negative or positive for that antibody. This could result in a potential false negative result for that assay for any patients tested in well H6.

- 50) **SonarMed AirWave Monitor, Class II** – Potential for the presence of two error codes which would make the monitor inoperable.
- 51) **BD Kiestra InoqulA+ Software Version 20.3. IVD automated specimen processing, Class II** – An anomaly is present in InoqulA / InoqulA+ software version 20.3, has the potential to cause a mismatch between a specimen and plate.
- 52) **syngo.CT software version VA48A_SP5.5, Class II** – SOMATOM Definition Edge, SOMATOM Definition AS, SOMATOM Definition Flash with software syngo.CT with Software version VA48A_SP5 may result in scanning workflow interruptions and unexpected user notifications. and may result in a delay in diagnosis and/or patient rescans.
- 53) **Fujifilm FDR Go Plus mobile X-ray system, Class II** – The graphics driver of the FDR Go PLUS might cause the appearance of a Blue Screen of Death (BSoD).
- 54) **MassHunter Quantitative Analysis Software, Class II** – When utilizing specific software versions of an LC/MS device, and Batch at a Glance in Compound Table view, a defect occurs when a new sample(s) is inserted. This defect creates a mismatch between the sample name and the column header whereby the sample header will be offset by one sample. The recalling firm requests that you discontinue using this workflow to generate reports because the Quant batch table will not display fully analyzed results or save any changes made.
- 55) **ACUSON NX2 Diagnostic Ultrasound System, Class II** – The action is being initiated due to internal testing which identified a possibility for transducers to exceed the acoustic output power (AOP) values defined. The transit voltage values based on PW Doppler are calculated normally but not loaded correctly into hardware.
- 56) **RayStation, Class II** – Isocenter shifts when using dose tracking in RayStation 3.5, RayStation 4.0, RayStation 4.5, RayStation 4.7, RayStation 5, RayStation 6, RayStation 7 and RayStation 8A. In these versions, isocenter shifts in dose tracking are incorrectly interpreted according to the DICOM patient coordinate system.
- 57) **ABL90 FLEX Analyzer, Class II** – Software Security; The action is being initiated because of software security vulnerabilities with the firm's analyzer operating system, which may cause the device to shutdown or reboot resulting in delayed medical treatment.
- 58) **QIASymphony SP SOW 5.0.3, software used with the QIASymphony SP Instrument, Class II** – QIASymphony software version 5.0.3 - Software issue

- incorrectly assigns the 2D bar code eluate ID to the sample within the results file. If 2D bar code eluate IDs are not checked against the sample ID prior to downstream application the incorrect tube may be selected and it could have the potential to lead to delayed results or incorrect patient reporting.
- 59) **SOMATOM Definition Flash, Class II** – Potential for four safety-related software issues impacting systems utilizing syngo.CT software version VB10A which may result in a scan abort.
 - 60) **WS80A Diagnostic Ultrasound System, Class II** – There is a potential for probes overheating when decreasing the Doppler SV (Sample Volume) size value set by the user in the Doppler Only mode.
 - 61) **Philips EPIQ and Affiniti Ultrasound Systems with software version 4.0, Class II** – There is a potential that the image of one patient could get unexpectedly moved into another patient's folder when the user is using the Edit functionality on the Patient Data Entry (PDE) screen of the device.
 - 62) **VITROS Chemistry Products Calibrator Kit 32, Class II** – Potential Unsuccessful Calibration Due to Software Anomaly in VITROS System.
 - 63) **Philips Azurion systems with software version R1.2 -Interventional Fluoroscopic X-ray system, Class II** – The cold restart of Azurion R1.2 systems may take up to 7 minutes if the system is connected to the mains power supply for more than 50 days, may result in a delay of treatment.
 - 64) **PulsioFlex Monitoring System, Class II** – The monitor displays an error message. The error message states: "internal error restart or service".
 - 65) **MAC VU360, Class II** – Two issues: 1) The MAC VU360 system may intermittently display an incorrect patient ID or visit number on the screen after scanning the patient's barcode. This may result in the ECG report being assigned to the incorrect patient. 2) The MAC VU360 may have the incorrect patient demographics appear on the patient banner. This may result in the ECG report being assigned to the incorrect patient.
 - 66) **Spacelabs Healthcare Smart Disclosure System, Model 92810, a component of the Intesys Clinical Suite, Class II** – Several reports were received that patient records were printed with the correct patient demographics but containing another patient's waveforms.
 - 67) **Elekta Unity, Image-Guided Radiation Therapy System, Class II** – The QA software solution to perform the MR to MV alignment check, does not display the stored MR to MV offset values. The user is unable to independently inspect the values during their QA.
 - 68) **Radrex Digital Radiography System, Class II** – Software malfunction; It was found when a user performs radiography using the wireless flat panel detector (FPD), a message window displays on the monitor stating image transmission was not completed and there was no image available. It also showed the "OK" button to reacquire image data from the FPD, and the "Cancel" button to cancel the acquisition. When the user selects the "OK"

button, the same message window appears. This prompted the user to repeat the same operation several times and finally select the "Cancel" button to quit the reacquisition mode.

- 69) **RayStation, Class II** – When calculating electron Monte Carlo dose with a very large number of histories, the dose calculation may be wrong.
- 70) **SOMATOM go.Top, Class II** – The potential sporadic performance problems may cause scanning workflow interruptions and unexpected user notifications resulting in diagnostic delay or need for patient rescan.
- 71) **Accu-Chek Connect Diabetes Management App, Class II** – Users with Android OS 8.0 and above may be unable to transfer values obtained on their meter to the App.
- 72) **Alinity ciseris System Control Module, Class II** – Abbott has identified an issue with all on market versions (v2.6.0 and v2.6.1) of Alinity ci series Software where incorrect results may occur after a system Stop due to the Alinity i re use of reaction vessels (RVs). This issue only occurs if the system is transitioned from Processing to Stopped to Idle.
- 73) **CardioLab/ComboLab Recording Systems, Class II** – Potential for failure of the patient leakage current test. There is a potential that if another device with electrical connectivity (e.g., ablation device, ECG monitor) fails, then the CLab II Plus Amplifier will not prevent an electric current from completing a circuit, which could cause an electrical shock to a patient.
- 74) **Alinity s System, Class II** – During in house Alinity s System assay testing, it was identified that there is a possibility of unexpected low RLU (Relative Light Units) values on sample results for all Alinity s assays. The issue could potentially lead to incorrect results for all Alinity s assays.
- 75) **Grab n Go Opti series VIPR system, Class II** – Limited access to flow settings as a result of the control knob having been rotated beyond its functional range.
- 76) **C2 Nerve Monitor, Class II** – Stryker C2 NerveMonitor's design and instructions may not optimally address usability issues related to the functionality of the device, which may result in use errors potentially causing or contributing to nerve injury.
- 77) **Monaco Radiation Treatment Planning System (RTP) System, Class II** – Monaco is displaying the Anatomy and Beam shift direction incorrectly on the Monaco Scan and Setup Reference Report and is DICOM exporting incorrect (Anatomy/Beam) shift directions.
- 78) **MiniMed 670G Insulin Infusion Pump, Class II** – Medtronic MiniMed is recalling the MiniMed 600 series insulin pump because it may become temporarily stuck, and the keypad becomes unresponsive.
- 79) **Centricity Universal Viewer 6.0, Class II** – There is the possibility of viewing studies directly from the Enterprise Archive or VNA with incorrect patient images because the updated series or study is not present in the archive.

- 80) **myCordella Patient Kit without ECG, Class II** – The firm have received reports of patients myCordella Hubs fully powering themselves down without interaction from the patient or Endotronix.
- 81) **Ingenuity TF PET/CT, Class II** – In certain instances when performing a cardiac step and shoot acquisition with phase tolerance selected, images may be labeled as if phase tolerance had been applied when phase tolerance had not been applied.
- 82) **Lantis system (pre-2003), Class II** – Potentially affected by the Microsoft Windows Remote Desktop Protocol (RDP) vulnerability.

Steven Mnuchin, Israeli Health Officials Discuss Establishment of Israeli FDA Branch

According to Calcalist, in October, the U.S. Secretary of the Treasury, Steven Mnuchin, met with Israeli health officials and Marius Nacht, co-founder of life sciences and healthcare venture capital fund aMoon, to discuss the opening of a local branch of the U.S. Food and Drug Administration. Here is the article:

<https://www.calcalistech.com/ctech/articles/0,7340,L-3772615,00.html>

FDA Moves to Electronic-Only Device Submissions

The FDA now requires medical device premarket submissions to be sent electronically, eliminating the need for multiple paper submissions. The guidance was issued on December 13, 2019. This guidance describes how the Food and Drug Administration (FDA) is implementing the eCopy Program under section 745A(b) of the FD&C Act. The inclusion of an eCopy is expected to improve the efficiency of the review process by allowing for the immediate availability of an electronic version for review rather than relying solely on the paper version.

<https://www.fda.gov/media/83522/download>

Off-The-Shelf Software Use in Medical Devices

The FDA released the updated Off-The-Shelf Software guidance on September 27, 2019. The previous edition of this guidance was released in 1999.

The detail of documentation to be provided to FDA and the level of life cycle control necessary for the medical device manufacturer increase as severity of the hazards to patients, operators, or bystanders from OTS Software failure increases.

From a practical point of view, the OTS software should go through the following process:

- 1) Identify the OTS in the device
- 2) Assess OTS LOC
- 3) Perform OTS software hazard analysis, including mitigations and residual risks

An OTS Software Report should be prepared for the FDA submission.

The updated guidance requires a risk analysis of the OTS software.

<https://www.fda.gov/media/71794/download>

IEC 62304 Update

The draft second version of IEC 62304 was released for review in October. The comments were received, and we should expect the updated draft to be released for review sometime the first half of 2020. Depending upon the comments in the updated release, we may finally see a release of Edition 2 of the IEC 62304 during 2020.

ISO 81001-1

The ISO 81001-1 standard, Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms, was released for review.

This document articulates the foundational principles, concepts, terms and definitions for health software and health IT system safety, effectiveness and security across the full life cycle, from concept to decommissioning.

Health software is considered software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device.

Health IT system is considered a combination of interacting health information elements (including health software, medical devices, IT hardware, interfaces, data, procedures and documentation) that is configured and implemented to support and enable an individual or organization's specific health objectives.

Do you have a question about FDA Digital Health Regulatory Policy?

The Digital Health Team at FDA/CDRH has open a resource for aiding companies. The resource is found at:

https://www.fda.gov/medical-devices/digital-health/ask-question-about-digital-health-regulatory-policies?utm_campaign=2019-11-06%20CDRH%20New&utm_medium=email&utm_source=Eloqua

Software Link Suspected in Airbus Engine Blowouts

Not only in medical devices – software strikes again!

According to Business Insider, a probe into a series of engine failures on Airbus's A220, is studying whether a software change set off unexpected vibrations that damaged fast-moving parts and forced three emergency landings. The article is found at:

<https://www.businessinsider.com/exclusive-software-link-suspected-in-airbus-a220-engine-blowouts-sources-2019-10>

ISO 14971:2019 Released

The standard ISO 14971:2019, Medical devices — Application of risk management to medical devices, was released in December 2019. The guidance on the application of this document can be found in ISO/TR 24971.3, which is under development and should be released next year.

Australia Medical Device Cybersecurity Guidance

Australia released the Medical Device Cyber Security Guidance for Industry in July 2019. The guidance is similar to the future guidance planned for by the FDA. <https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf>

FDA Recognizes ANSI/AAMI/UL 2800-1:2019 as Consensus Standard

The FDA has recognized AAMI/UL 2800-1: Standard for Safety for Medical Device Interoperability, as a consensus standard on 15 July 2019. The standard specifies a baseline set of requirements for assuring safe and secure interoperability for Interoperable Medical Systems.

URGENT/11

A security firm has identified 11 cybersecurity vulnerabilities, named "URGENT/11." The FDA, on 1 October 2019, issued a safety communication called URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party

Software Component May Introduce Risks During Use of Certain Medical Devices.

The “URGENT/11” set of 11 vulnerabilities pertain to IPnet, a third-party communications software component found in a variety of medical device types, and could enable outside parties to commandeer devices and alter their functions or disable them, according to a safety communication from FDA.

<https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce>

FDA’s Role in Cybersecurity for Medical Devices

The FDA has issued a Fact Sheet titled: The FDA’s Role in Medical Device Cybersecurity. This fact sheet dispels certain myths and explains what it is really about.

<https://www.fda.gov/media/123052/download>

CE - Cybersecurity

Various Notified Bodies (NB) have been asking to see what is being done for cybersecurity, citing the FDA’s guidelines (as the CE does not yet have any explicit guidelines for cybersecurity covered in the MDD).

For software only projects, the NBs have been citing EN 82304-1:2017 which relates to health software and the security aspects of running on a network.

The MDR (EU-Regulation (EU) 2017/745), defines, in Annex I, various references to the following cybersecurity issues:

14.2(d) the risks associated with the possible negative interaction between **software and the IT environment** within which it operates and interacts.

17.2 For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including **information security**, verification and validation.

17.4 Manufacturers shall set out minimum requirements concerning hardware, **IT networks characteristics and IT security measures**, including protection against unauthorised access, necessary to run the software as intended.

Principles and Practices for Medical Device Cybersecurity

The IMDRF (International Medical Device Regulators Forum), Medical Device Cybersecurity Working Group, issued on 1 October 2019, a draft document titled: Principles and Practices for Medical Device.

<http://www.imdrf.org/docs/imdrf/final/consultations/imdrf-cons-ppmdc.pdf>

General Wellness

The FDA has issued the General Wellness: Policy for Low Risk Devices Guidance on 27 September 2019. The guidance is a compliance policy for low risk products that promote a healthy lifestyle (general wellness products).

<https://www.fda.gov/media/90652/download>

Medical Device Data Systems - MDDS

The FDA has issued an updated guidance on Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices Guidance on 27 September 2019.

A MDDS does not modify the data or modify the display of the data, and it does not by itself control the functions or parameters of any other medical device. The FDA has decided that MDDS pose a low risk to the patient, the FDA does not intend to enforce compliance with the regulatory controls that apply to MDDS.

<https://www.fda.gov/media/88572/download>

21st Century Cures Act Changes

The FDA issued on 27 September 2019 the Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act. This guidance provides FDA's current thinking regarding the amended device definition and the resulting effect the amended definition has on FDA's guidances related to medical device software.

<https://www.fda.gov/media/109622/download>

Clinical Decision Support Software

The FDA has released the Clinical Decision Support Software Draft Guidance on 27 September 2019. It is being distributed for comment purposes only. This guidance provides clarity on the scope of FDA's oversight of clinical decision support software intended for health care professionals, patients, or caregivers.

<https://www.fda.gov/media/109618/download>

FDA's Software Related Prioritized Medical Device Guidance Documents to Publish in FY 2020

A-List Final Guidance Topics:

- Safer Technologies Program for Medical Devices
- Clinical Decision Support Software

A-List Draft Guidance Topics:

- Content of Premarket Submissions for Cybersecurity of Medical Devices
- Computer Software Assurance for Manufacturing, Operations, and Quality System Software

B-List Draft Guidance Topics:

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

It's imperative to see the direction that the FDA is going with software regulation. The emphasis will be on handling clinical decision support software (until now this type of software has mainly flown under the radar), upgrades in cybersecurity requirements and software used in the organization (bring the FDA in line with ISO 13485:2016).

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.

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