# Medical Devices recalled due to Software and Hardware faliure and Cyber-Security Issues

Authors- Hemant Vardani, Yash Agrawal , Aman Jain

***Abstract*— Smart healthcare is an integral part of smart cities. Modern medical devices are becoming increasingly software dependent. Doctors and patients are now using their smart-phones to control and monitor implantable medical devices (IMDs) such as cardiac implants, insulin pumps, deep brain neurostimulators, etc via the Internet or Bluetooth connections.Internet of Things (IoT) is major invention of recent few decades.When these smart devices or internet connected devices are interact together, then they create a cyber infrastructure. Such connectivity expands the devices' ability to fulfill healing and diagnostic functions in a quick and cost-effective manner and can help save many live. As these are life critical systems, each and every component should perform its task as required till the purpose is fulfilled. In many cases it is seen that due to hardware or software the medical devices issues the purpose of device is not fulfilled, in that case its necessary to recall such devices as soon as possible before a serious condition occur like injury, infection or even death to patient or the medical staff like doctor or the operator of the device. So it is need to check the system in all the aspect of situation by the hardware team and more importantly the software team. But as the reliability is increasing on the software also results in exposure to several security threats. Control of such devices via the underlying communication network may allow attackers to exploit the critical system vulnerabilities of these devices. Attackers could manipulate the settings of these devices and may try to harm the patients and these malicious attacks can originate from anywhere in the world. However, there have been very few real attempts to hack such devices and harm patients. We investigate the practical security risks involved with the use of IMDs and also the critical issues faced by medical cyber physical system(medical CPS) in current era which we require to overcome in future to provide efficient and reliable service to patients and the medical staff or the operating head, as to save more and more life.**

***Index Terms*— Cyber Physical system, Cybersecurity, Medical Devices, Recalls, Software Failure, Hardware Failure, Attacks, FDA.**

**/organization/pubs/ani_prod/keywrd98.txt**

## I. Introduction

Cyber Physical System playing its vital role for mankind via designing software and hardware related medical devices. Day by day as humans are exploring their hands on new technologies, along with major breakthroughs and discoveries, the complexities of program and design is keep on increasing. The important thing to note is that device complexity isn't necessarily always good. Rather they become prone to bugs and errors. Hence it has been seen since 2011 software and hardware devices recalls were made on large scales every year because these medical devices subjected to faults are non-negligible because it can lead to potentially catastrophic impacts on patients. In a 2011 research it was stated that most medical devices recalled in the last five years for "serious health problems or death" had been previously approved by the FDA using the less stringent, and cheaper, 510(k) process. This was by Dr. Diana Zuckerman and Paul Brown of the National Center for Health Research.

This paper submitted on 15 October 2021. We want to thank Dr. Ashish Sharma, Assistant Professor at Indian Institute of Information Technology KOTA ,who supported and motivated us for this paper.

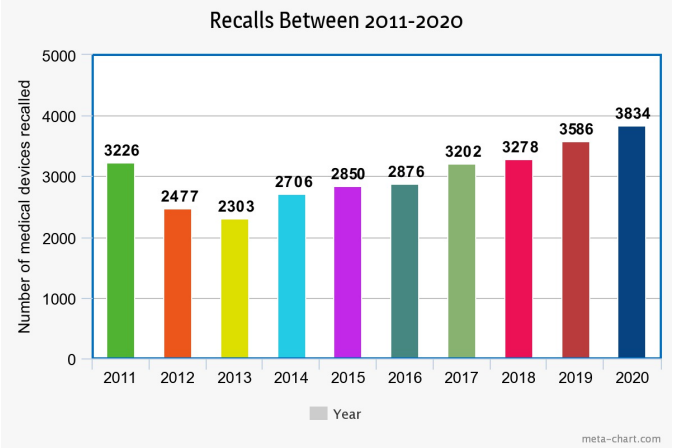


Fig. 1. Survey of medical devices recall between year 2011-2020 as per the data provided by FDA.

### A. Analysis of trend of 2011-2020 year

This statistic shows the leading causes of medical device recalled globally during the period 2011-2020. For this time period, the main cause of recall for medical devices was in the area of device design, with a yearly average of 3,034 such recalls over the period 2011-2020. During the phase of covid highest number of medical devices recalled 3834 registered while 2303 medical devices recalled in 2013 is smallest but afterwards the graph continuously increasing.

### B. Classification on the basis of Risk Of Injury

Classification on the basis of Risk Of Injury

Class I: It is a situation in which usually pertain to defective products, there is a reasonable probability that the use of exposure, to violative product will cause serious adverse health consequences or death. Products such as pacemakers,heart devices,contamination from toxin and lifesaving drugs fall into this category.

Class II: It is a situation in which use of exposure to a violative product issues held can cause temporary or medically reversible adverse events or where the probability of serious adverse health consequences is remote. It is also called as Short-term health issue because there is a slight chance it could lead to a serious problem.Many medical implants,such as hips or knees, fall in this category.

Class III It is a situation in which use of exposure to a violative product apply to cause minor product defects or errors that are unlikely to cause harm to someone's health. These products are not likely to cause injuries.There are very few examples such as implantable pacemakers and breast implants.

### C. Reasons of failure

The failure occurring, due to which later recall cost has to be borne, may occur due to many reasons.

**Survey of Medical devices recalled software and hardware issues.**

Displaying year of Recall and Number of recall as per fda data

| SNo. | Device Name | Company | Diseases | swhw | Year | No. of recalls | Reason |
|---|---|---|---|---|---|---|---|
| 1 | AMSORB PLUS PREFILLED C-CAN 1.0L | Armstrong Medical Limited | Anesthesia | hw | August 5, 2021 | 214,032 | Reduced Gas Flow to Patients During Anesthesia |
| 2 | Argyle IVC Insertion Tray | Cardinal Health | UVC | hw | June 16, 2021 | 7,197 | Missing Instructions for Use for the Safety Scalpel #11 |
| 3 | Continuous and Non-Continuous Ventilators, including CPAP and BiPAP | Philips Respironics | Sleep Disorders | hw | June 14, 2021 | 514,037 | Risk of Exposure to Debris and Chemicals |
| 4 | INGENIO Family of Pacemakers and CRT-Ps | Boston Scientific | Low heart rates | sw | June 3, 2021 | 48,000 | Risk of Transition to Safety Mode |
| 5 | Lex SARS-CoV-2 Assay (M128) | Quidel | Covid-19 | sw | April 26, 2021 | 18385 | Risk of False Negative Results |
| 6 | Arid Medical | Medical Convenience Kits | Surgical Care | others | April 2, 2021 | 1,570 | Risk of Fungal Contamination |
| 7 | Alaris Infusion Pump Module 8100 Bezel | Step-Har Medical | Medical care | hw | February 26, 2021 | 2 | Possible Cracked or Separated Bezel Repair Posts |
| 8 | Fixed Core Wire Guides, | Cook Medical | Serious Injuries | hw | October 14, 2020 | 61 | Device Damage from a Manufacturing Error |
| 9 | Trevo XP ProVue Retriever | Stryker Neurovascular | Accident | hw | September 21, 2020 | 1,258 | Core Wire That May Break or Separate During Use |
| 10 | Medfusion 3500 and 4000 Syringe Pumps | Smiths Medical | General | sw+hw | June 26, 2020 | 46,395 | Risk of Medication Delivery Error |
| 11 | BodyGuard Infusion Pump System | CME America | Infusion & Outfusion | hw | January 7, 2020 | 28,448 | Risk of Over-, and Under-infusion |
| 12 | CARESCAPE Respiratory Modules | GE Healthcare | Anesthesia | sw | September 27, 2019 | 165 | Incorrect Oxygen Values |
| 13 | King Vision Video Laryngoscope Adapter Size ¼ | King Systems | Patient Upper airway and aid | sw | November 5, 2019 | 107 | a Display of The Reversed Image |
| 14 | GlideScope Core One TrueSteam Cable ("OneTouch cable") | Verathon, Inc. | Airway and Vocal Cords | sw+hw | May 6, 2020 | 356 | partial or complete loss of image during use |
| 15 | Langston Dual Lumen Catheter | Vascular Solutions, Inc. | Angiography | hw | March 16, 2020 | 4,304 | Risk of Separation During Use |
| 16 | Ovation IX Abdominal Stent Graft System | Endologix Inc. | abdominal aortic or aortoiliac aneurysms (AAA), | hw | May 6, 2020 | 5,403 | Risks of Polymer Leaks During Implantation |
| 17 | VNS Therapy SenTiva Generator | LivaNova | VNS Therapy | sw | August 22, 2019 | 2909 | Reset Error |
| 18 | ROSA Brain 2.0 Robotic Surgery System | Zimmer Biomet | Neurosurgeons | sw | September 10, 2019 | 86 | Software Issue that Incorrectly Positions the Robotic Arm |
| 19 | Circular Staplers | Ethicon | Gastrointestinal Tract | hw | April 11, 2019 | 92,496 | Inefficient Firing and Failure to Completely Form Staples |
| 20 | Swan-Ganz Thermodilution Catheter | Edwards Lifesciences | Blood Pressure | sw+hw | December 21, 2018 | 1,426 | Incorrect Assembly Causing Reversal of Lumens |
| 21 | CPAP Mask Cushion Devices | Compass Health Brands | obstructive sleep apnea | hw | May 22, 2018 | 742 | Possible Air Leaks |
| 22 | CoaguChek XS PT Test Strips | Roche Diagnostics | warfarin | sw | September 13, 2018 | 1.1 million+ | Inaccurate INR Test Results |
| 23 | MindFrame Capture LP Revascularization Device | Medtronic | ischemic stroke | hw | February 26, 2017 | 529 | Wire Material That May Break or Separate During Use |
| 24 | Fabius Anesthesia Machines | Dräger Medical | Anesthesia | other | March 1, 2018 | 62 | Production Step Error |
| 25 | AirLife Humidification Chamber & Heated Breathing Circuit Kits | Vyaire Medical | serious diseases | other | November 29, 2017 | 16,670 | Manufacturing Error |
| 26 | Certitude Delivery System | Edwards Lifesciences LLC. | transcatheter aortic valve replacement | hw | July 21, 2017 | 1,730 | Certitude Delivery System |
| 27 | NeuroBlate System | Monteris Medical | brain tissue | sw+hw | October 5, 2017 | 52 | Unexpected Heating of Laser Delivery Probes |
| 28 | SERIS exoMAG Magnetic Silica and NeoSEDIS Magnetic Extraction Reag | bioMerieux | molecular genetics assays | sw+hw | November, 23 2016 | 376 | Potential Inaccurate Test Results |
| 29 | Coronary Catheters | Abbott Vascular | cardiac | hw | March 22, 2017 | 132,040 | Risks Stemming from Difficulty Removing Balloon Sheath |
| 30 | LeadCare Plus and Ultra Testing Systems | Magellan Diagnostics Inc. | lead in blood | sw | April 12, 2017 | 1,089,984 | Inaccurate Test Results |

Fig. 2. Medical devices recalled as per the data provided by FDA. **https://rb.gy/qqyyad**

The major reason is lack of coordination with control software components and the UI software. Another can be incorrect or missing interaction options or on-screen instructions. These errors

are related to providing the user with poor options and instructions to interact with devices. Some known cases of poor design or configuration of alarm functionalities also played detrimental role in failure of devices. Alarms have been adopted by most devices as an important safety feature attracting user attention to critical events, such as deterioration of patient condition or device failures. Even some other instances of causing errors are also observed such as immature timeout mechanisms for user inactivity and to configure devices incorrect data have been used.

Other categories of error are associated with Output Render like instance any medical images might be displayed in an incorrect size, format, quality, or color. In many types of devices, medical images are an important type of feedback on which users (e.g., radiologists, oncologists) rely to correctly diagnose and treat patients. Even Incorrect rendering of on-screen widgets can be a cause. On-screen widgets include device controls (e.g., soft buttons), input components (e.g., text fields), and navigational tools (e.g., scroll bars) necessary for the user to operate the device and browse the information presented on the display.

## II. Analysis of above table

Table lists example keywords from the dictionary we used to identify computer-related failures in each fault class. The Software class represents failures due to software errors. The Hardware category includes both electrical issues and defects of internal circuits, whereas the I/O category includes failures due to sensors, connections, display, or speakers. In this we actually discuss that a medical device failure can be occurs from every company either is big or small there are lot of medical devices recalled due to some reasons faces various diseases every year.

### A. Case study I

Lets go and dive into a case study to get a closer overview.

NeuroBlate Laser Delivery Probes are small, carbon dioxide (CO2)-cooled catheters that allow minimally invasive entry into a patient's brain. The probes are part of the Monteris Medical NeuroBlate System, which is used during surgical procedures to remove (ablate), thicken or solidify (coagulate), or destroy (necrotize) cells in brain tissue. But due to some reasons it was listed in class I category of FDA and in some cases, the NeuroBlate Laser Delivery Probes interact with the MRI system used to visualize the position of the catheter and cause unexpected heating and damage to the tip of the probe. This could cause unanticipated heating of surrounding brain tissue, or damage the tip of the probe, and allow the CO2 cooling gas inside the probe to leak into the brain. Until appropriate mitigation strategies have been identified by the manufacturer and evaluated by the FDA, the FDA recommends health care providers should strongly consider treating patients using alternative procedures if available. Health care providers who do not believe there is a viable alternative should use the device with extreme caution. Affected Patients those who undergo brain tissue ablation and neurosurgeons who may be using these devices.

### B. Case study II

Now take a look into the other case:

The Alaris System is an infusion pump and vital signs monitoring system recalled in January 2020. The pump provides fluid,blood & blood products through an infusion tubing set into a patient's vein or through other cleared routes of administration. The device is used in adult, pediatric and neonatal care. But due to some reasons it was listed in class I category of FDA like system errors, delay options programming, low battery alarm, keep vein open(KVO) "end of infusion" alarm priority.This errors can lead to delay in infusion ,interruption of fusion,slower than expected delivery of medication(under infusion), and faster than expected delivery of medication(over infusion) due to this health care providers,patients having infusions using the Alaris System.There have been serious adverse health events with each of these errors. There are 55 reported injuries and one death. BD/CareFusion 303 will contact all affected customers to begin the scheduling process for the software update when the software becomes available. Consumers with Alaris System Infusion Pumps System Software 9.33 and earlier should follow these specific recommendations to help mitigate the potential risk of errors until the software issues have been remediated.

## III. Security Issues in the Medical-IOT CPS Domain

### A. Security Attack in Medical Devices operating on medical CPS

**1] Stuxnet :** Stuxnet is a computer worm that exploits many of the previously unknown Windows zero-day vulnerabilities to infect computers and PC's. The main aim of this Stuxnet was to cause real-world physical effects. By targeting centrifuges, it used to produce the enriched uranium that powers nuclear devices, weapons and reactors. The U.S. and Israeli governments created the worm as a tool to derail and delay the Iranian program to develop nuclear weapon technology.

**2] Distributed Denial of Services (DDoS):** A distributed denial-of-service (DDoS) attack is a malicious attempt to destroy normal traffic of a particular server, service or network. They mainly achieve effectiveness by making use of many computer systems as sources

of attack traffic. Some recent DDoS attacks are those of GitHub and DYN which took down GitHub for around 20 mins.

**3] Man in the Middle Attack:** An MITM (SSL Hijacking) attack is a type of hacker hijacking that occurs when the hacker himself intercedes the communication between the server and the client. It executes the hack by substituting the IP address of the hackers' computer with that of the client's and hence deludes the server. The server continues to communicate with the hacker assuming that it is the true client. A British couple lost £340,000 in an email eavesdropping/ email hijacking MITM attack which was indeed a fatal loss for them.

**4] Phishing Attack:** It involves the practice of sending emails which appear to be from trusted sources but actually intends to load some malicious malware into the target system without the knowledge of the client in the form of a mail attachment or any other plausible source. This can be minimized with the help of sandboxing- a technique used for testing the email content before its put into use

**5] Insider Attack :** It is considered as an attack executed by a professional who has authorized system access and hence, he or she can be tagged as a traitor. They intend to attack all computer security elements and range from implanting Trojan virus in the network to stealing sensitive data

### *B. Security Issues in Medical Devices operating on medical CPS*

**1] Risk of wireless communication:** Security vulnerabilities in these devices can be exploited to attack a patient's Such IMDs often come coupled with an intermediate gateway device which can wirelessly connect to the implanted device, periodically log patient information and share it with concerned medical personnel through the Internet/cloud based storage to enable remote patient monitoring with great ease and convenience. In addition to intermediate gateway devices, IMDs may also be controlled with smartphones or personal computers. Lack of proper measures to ensure secure data storage in the gateway device, smartphone, personal computers, or cloud storage facilities, and insecure data transmission between any of these devices can also lead to various security risks (Yaqoob et al., 2019).

**2] Electromagnetic Interferance**: There are two main strategies that an adversary might adopt: (1) by targeting frequency that lies within the sensor's frequency band (base-band EMI attacks), or (2) by targeting frequency just outside the base-band (amplitude modulated EMI attacks). The analog sensors in these medical devices can be affected by intentional EMIs under 10W, which can inhibit pacing and induce defibrillation shocks from distances up to 1 -2 meter in free air. For example, baseband attacks on cardiac IMDs can deliberately manipulate electrocardiogram (ECG) readings of an IMD and prompt it to deliver possibly fatal defibrillation shocks.

**3] Unintentional risks of IMD:** Battery Leakage:A decrease in battery capacity could cause unexpected failures or premature shut-downs resulting in serious con-sequences for the patient. Soft-ware patches/updates : After finding security flaws/bugs in device firmware, manufacturers may push patches/updates to their IMDs to improve device functionality and security. infections:The clinical standard for SIRS includes the presence of at least two of the following four symptoms (Kalil, 2019). •Body temperature lower than 96.8 F or higher than 100.4 F. •Heart-beat higher than 90/min. •Breath-rate higher than 20/min. •White blood cell count is lower than 4000/uL or higher than 12,000/uL.

**4] Security based-classification:** The Federal Drug Administration (FDA) provides cybersecurity guidance for the premarket stages of medical device development. The European Union's Regulation for Medical Devices also discusses cybersecurity requirements for premarket and post-market stages. These regulations classify medical devices into four categories (I, IIa, IIb, and III). It is important to note that these classifications are applied to med-ical devices in general and not exclusively for IMDs.

### *C. Solution for Attacks faced by Medical Devices*

In the past few decades it is noticed that due to advancement in technology we humans are now trying to make use of body sensor networks or wireless scan of body area to reduce the amounts of wire connections and physical inputs required. Intrusion Detection Systems (IDS) are used to identify the hacker patterns and the algorithms used to destroy the CPS in medical field. However, the installation of IDS is a difficult task as it is hard to connect to Medical CPS actuator systems. Earlier even homomorphic encryption was put into implementation. It is a basic form of encryption which mainly allows computation and processing on cipher-texts and data and generates an encrypted result, which on decryption would match the result of the operations as if they were performed on the plain text.

### *D. Tools and Mechanisms for Detecting These Attacks*

Hyper Network Model of Statistical Analysis System, It has a simple structure with a protection scheme and other functions usually in use for other types of transmission substations.

Each function consists of multiple Logical Nodes. A Logical Node is a sub-function located in a physical node, which exchanges data with other separate logical entities.

It acquires data from current transformers and voltage transformers, and calculates the measurands.

In the hyper-network model of SAS, a function which consists of a set of logical nodes, a hyper-edge participates in multiple functions and is more generic and helps in identifying the critical data retrievers.

## IV. Future of medical CPS in life of humans

CPS in the medical field is only in its gradually developing stage itself can be considered as one of the main platforms for developing and innovating ideas in this field. The ideology of interdisciplinary approach integrating robotics, Artificial Intelligence (AI) and medical knowledge together increases the precision and accuracy rates and help in increasing the efficiency of the CPS. Opportunities for future research in CPS can be as: achieving reliability via a dedicated middle ware, component based reasoning for performance improvement and flexibility by adopting the aspect-oriented programming model, portable agents. Further, we find that most of the research challenges (listed in section VI) are mostly unsolved and we believe that future research in these areas can provide an additional level of security to respective CPS/ Medical CPS.

## V. CONCLUSION

Product recalls will always be challenging for any medical device manufacturer, hence it becomes indispensable to minimize the num-ber of recalls. The basic idea is to manufacture the product with correct and focused information security processes, reporting and feedback loops, risk management, regulation, resilience activities, and international standards( like ISO/IEC 27032:2012 , IEC 62304:2006, IEC/ISO CD 82304 which are must to be followed). These are best technical controls methods. Next move can be if the need to recall has

been recognized then proper set of analytics, alerting, and reporting capabilities combined with proven supply chain execution systems that provide visibility across the supply chain, medical device OEMs can enhance their recall management capabilities and improve the quality of their response. This can be major differentiable move toward either life or death.

The awareness of cyber security vulnerabilities in medical devices has also become the need of the hour. Therefore to tackle the challenge it is must to understand the cyber security vulnerabilities that are already present in their networked medical devices, including the potential exposure of sensitive information and the associated. The design and development process should be formulated keeping in view cyber security protection. Standards revision and new national guidance is currently addressing this objective. Accountability for medical device cyber security, using standards, to assist manufacturers and implementers, together with regulatory oversight to ensure compliance must be assured. Therefore, the medical device industry advocacy must assist in promoting increased awareness of cyber security and privacy issues.

## References


[1] https://meridian.allenpress.com/bit/article/47/6/514/142716/Software-Related-Recalls-An-Analysis-of-Records.

[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5518627/

[3] https://sci-hub.ren/https://www.sciencedirect.com/science/article/abs/pii/S2210670720307708

[4] https://www.sciencedirect.com/

[5] https://ced.ifmbe.org/blog/ifmbeced-machinelearning-clinicalengineering.html

[6] https://rucore.libraries.rutgers.edu/rutgers-lib/64635/PDF/1/play/

[7] https://www.sciencedirect.com/science/article/abs/pii/S2210670720307708

[8] https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050920X00032/1-s2.0-S1877050920300673/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEKr

[9] https://rucore.libraries.rutgers.edu/rutgers-lib/56984/PDF/1/play/

[10] https://www.sciencedirect.com/science/article/abs/pii/S2210670720307708

[11] *https://www.sciencedirect.com/science/article/pii/S1877050920300673*

[12] https://www.sciencedirect.com/science/article/abs/pii/S2210670720307708

[13] https://www.sciencedirect.com/science/article/abs/pii/S2210670720307708

[14] https://sci-hub.hkvisa.net/10.1109/ICECCS.2017.20

[15] https://sci-hub.hkvisa.net/10.1109/jproc.2011.2161241

[16] https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/227466

[17] https://www.taylorfrancis.com/books/mono/10.1201/9781420042238/medical-device-reliability-associated-areas-dhillon

[18] https://www.worldscientific.com/doi/abs/10.1142/S021853930100058X

[19] https://onlinelibrary.wiley.com/doi/abs/10.1002/smj.2340

[20] https://www.fda.gov/medical-devices/medical-device-safety/medical-device-recalls

[21] https://www.statista.com/topics/3102/pharmaceutical-and-medical-device-recalls/

[22] https://www.statista.com/study/38527/pharmaceutical-and-medical-device-recalls-statista-dossier/

[23] https://www.medtechintelligence.com/featurearticle/trends-in-medical-device-recalls/

[24] https://bmjopen.bmj.com/content/1/1/e000155

[25] https://www.fda.gov/medical-devices/postmarket-requirements-devices/recalls-corrections-and-removals-devices

[26] https://www.fda.gov/about-fda/cdrh-transparency/overview-medical-device-classification-and-reclassification

[27] https://www.fda.gov/medical-devices/emergency-situations-medical-devices/coronavirus-covid-19-and-medical-devices

[28] https://link.springer.com/article/10.1007/s00521-021-06219-9

[29] https://www.emerald.com/insight/content/doi/10.1108/IJHG-08-2020-0090/full/html

[30] https://www.sciencedirect.com/science/article/abs/pii/S0883944120307358

[31] https://www.bmj.com/content/342/bmj.d2822.full

[32] https://ieeexplore.ieee.org/abstract/document/6509886

[33] https://sci-hub.ren/https://www.sciencedirect.com/science/article/abs/pii/S088394412030

[34] https://instanano.com/download-research-papers-books/

[35] https://rb.gy/qqyyad