International Journal Dental and Medical Sciences Research
Volume 5, Issue 5, Sep-Oct 2023 pp 335-337 www.ijdmsrjournal.com ISSN: 2582-6018

The locked AICD [automatic implantable cardioverter defibrillator]

Dr Anish Chugh, Dr Dhiraj Kumar, Dr Ajay Mahajan
D.M. Cardiology Resident
Asst Prof. Dept. of Cardiology Seth G.S. medical College and K.E.M. Hospital
Prof. & H.O.D. Dept. of Cardiology Seth G.S. medical College and K.E.M. Hospital

Date of Submission: 01-10-2023 Date of Acceptance: 10-10-2023

ABSTRACT
We present a case report of Cardiovascular Implantable Electronic Device [CIED] malfunction in a 38-year-old female implanted with automatic implantable cardioverter defibrillator [AICD] which had 17 episodes of high voltage charging leading to loss of battery life sending the device into back up mode with shock therapy being disabled and requiring replacement after explanation . This case highlights the importance of regular follow-up, timely interventions and regular periodic device interrogations in patients with Cardiovascular Implantable Electronic Device [CIED]

Keywords: Locked automatic implantable cardioverter defibrillator [AICD], Back up mode, Cardiovascular Implantable Electronic Device [CIED]

Presentation of case

A 38-year-old female with Doubly committed Right Ventricle with hypothyroidism with severe RV dysfunction and normal LV function had undergone corrective surgery in 2010, seven years later developed scar related Ventricular tachycardia for which she underwent a single chamber AICD implantation [2/2/18]. She received multiple device delivered appropriate shocks requiring electrophysiological study and radiofrequency ablation. And was sent home on oral Mexiletine, Warfarin, Amiodarone, Metoprolol succinate, Spironolactone, Furosemide and Thyronorm. On her visit for annual follow up the AICD device was found to be in VVI back up mode and was locked for further interrogation or programming. She had no indications to suggest an early battery depletion nor did she undergo MRI so as to interfere in device function. On device interrogation the cause of events could not be identified hence the manufacturer provided another device for replacement and perform a detailed analysis post extraction of previous unit. Detailed device image data analysis found the Fortify Assura device went into backup mode, due to a Power-On-Reset (POR).

The device had undergone 17 charging events on the day the reset and backup occurred. The POR and backup events were due to the multiple consecutive HV charging events, which loaded down the battery voltage.

The internal battery voltage measured 1.57V (below End of Service (EOS) level). After the device was recovered from backup VVI, electrical and functional tests performed did not identify any anomalies. Impedance measurements, telemetry, the device sensing, pacing, High Voltage (HV) charging, and therapy delivery functions were tested and found to be normal. she had to undergo AICD device replacement within 4 years of previous implantation whilst retaining old leads.

Follow-up: The patient has come for follow up with good lead and device parameters and a healthy surgical wound.

I. DISCUSSION:

In certain situations, the programming of an ICD is automatically changed to basic VVI back up mode. This mode can be viewed as a safety response to any errors encountered by the device in software or hardware. The device activates a reset function that attempts to overcome the error and restore normal operation if unsuccessful, the ICD may reset to VVI backup mode. ICD from all manufacturers have this function, which is intended to protect the patient from arrhythmic death even in cases of errors in ICD. The device resets to one therapy zone [a VF zone] and only shock therapy [no ant tachycardia pacing]. When an AICD enters back up mode most data stored in ICD are lost and settings during backup mode are non programmable.[1]

International Journal Dental and Medical Sciences Research
Volume 5, Issue 5, Sep-Oct 2023 pp 335-337 www.ijdmsrjournal.com ISSN: 2582-6018

Table 1 Selected parameters of the backup mode of most recent ICD models from St Jude Medical, Medtronic, Biotronik, and Boston Scientific (for further details, consult the user manuals available online)

	St Jude Medical	Medtronic	Biotronik	Boston Scientific
Backup called	Backup VVI/defibrillation only	Reset	Backup mode	Safety mode
Pacing mode	VVI	VVI	VVI	VVI
Pacing rate	67	65	70	72.5
SVT discrimination	Off	Off	Off	Off
Zones	1	1	1	1
VF rate	>146	>187	>170	>165
Detection	12 intervals	18/24	12/16	1 s
Redetections	6 intervals	12/16	12/16	1 s
Max sensitivity*	0.3 mV	0.3 mV	0.8 mV	0.25 mV

*Apart from max sensitivity, a number of other parameters is programmed to ensure proper sensing during VF. These parameters are also changed during VVI backup mode. Since they are unique to each manufacturer, a detailed explanation is beyond the scope of this manuscript.

The reasons causing the devices to enter back up mode can rarely be established, but are most often of technical character and completely unrelated to patient's medical condition. The backup mode balances 2 needs 1] ensure ICD therapy during life threatening ventricular arrythmias and 2] avoid inappropriate shocks [1]

In August 2016 Muddy Waters LLC released a report claiming that certain St. Jude Medical/Abbott cardiovascular implantable electronic devices (CIEDs) were vulnerable to cyberattack through the Merlin@home™ radiofrequency (RF) remote monitoring system. In January 2017 the United States Food and Drug Administration (FDA) released a statement providing information and making recommendations to reduce the risk of patient harm due to cybersecurity vulnerabilities. The FDA confirmed that an altered Merlin@home RF communicator could be used to modify programming commands to the CIEDs, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks. In response, on January 9, 2017, St. Jude Medical/Abbott issued a software patch for the Merlin@home RF communicator to reduce cyberattack vulnerabilities. It is believed that this patch was successfully programmed in nearly 100% of actively used Merlin@home RF communicators. On August 29, 2017, St. Jude Medical/Abbott released CIED firmware updates to reduce cybersecurity vulnerabilities among their RF-enabled pacemakers, including cardiac resynchronization therapy pacemakers and on April 17, 2018, St. Jude Medical/Abbott released firmware updates to strengthen cybersecurity performance in their line of RF-enabled implantable cardioverter-defibrillators (ICD) and cardiac resynchronization therapy defibrillators. Updating the CIED firmware requires an in-person manual device interrogation, takes approximately 3 minutes to complete, and is associated with a low risk of firmware update–related complications including palpitations, pocket stimulation, general discomfort, and failure to complete the update with the device remaining in backup mode. [2,3,4]

In 2020 Saxon and colleagues[4] published updated frequency and safety data regarding St. Jude Medical/Abbott cybersecurity firmware updates. They found that overall only 24% of active CIEDs had updated firmware and that globally a total of 9 pacemakers (9/220,500) and 8 ICDs (8/196,800) required replacement as a result of irreversible reversion to backup mode with loss of defibrillation or pacing programmability as a result of the firmware update procedure. They found that pacemaker dependency was independently associated with a lower likelihood of firmware update, which the authors concluded was "justifiable in light of the small number of devices that required replacement due to non-programmability and backup mode pacing." Further, the authors concluded that "deferring an update is a justifiable decision as there have been no reported cybersecurity breaches impacting the devices included in any of the FDA advisories to date." [5]

The worldwide frequency of CIEDs resetting to hardware/backup mode in response to the Merlin@home RF communicator among ~83,000 Ellipse, Fortify Assura, and Quadra Assura ICDs followed in the Merlin@home system was 0.30% [6]

II. CONCLUSION

Software glitches can cause a lot of problems in smooth functioning Cardiac implantable electronic devices [CIED] as evidenced whilist performing firmware upgrades or multiple High Voltage charges in our case, thus

hampering provision of appropriate care. Such issues can be minimized by Regular, meticulous, follow ups along with timely intervention to minimize the chances of adverse outcomes due to software mor hardware malfunction.

REFERENCES

[1]. Philbert, Berit & Tfelt-Hansen, Jacob & Jacobsen, Peter & Pehrson, Steen & Svendsen, Jesper & Jons, Christian & Petersen, Helen. (2016). Is modification of the VVI backup mode in implantable cardioverter-defibrillators from St Jude medical required due to increased risk of inappropriate shocks?.Europace. 19. euw083. 10.1093/europace/euw083.

[2]. Abbott Clinical update https://www.cardiovascular.abbott/content/dam/bss/divisionalsites/cv/pdf/reports/cyber_clinical_update_nov2019.pdf

[3]. A.Baranchuk, B. Alexander, D. Campbell, et al.Pacemaker cybersecurity: local experience with a firmware upgrade Circulation, 138 (2018), pp. 1272-1273

[4]. B.Alexander, V. Neira, D. Campbell, et al.Implantable cardioverter-defibrillator-cybersecurity CircArrhythmElectrophysiol, 13 (2020), pp. 277-279

[5]. L.A. Saxon, N. Varma, L.M. Epstein, L.I. Ganz, A.E. Epstein Rates of adoption and outcomes after firmware updates for Food and Drug Administration cybersecurity safety advisories CircArrhythmElectrophysiol, 13 (2020), pp. 869-872

[6]. Abbott Product Performance Report. 2020. Second edition https://www.cardiovascular.abbott/content/dam/bss/divisionalsites/cv/hcp/products/product-performance-reports/documents/Abbott-Product-Performance-Report-2020-Second-edition.pdf