Pacemaker firmware update and interrogation malfunction

Justin Z. Lee, MBBS,* Mark J. Henrich, RN,† Paul Bibby, RN,* Siva K. Mulpuru, MD,* Paul A. Friedman, MD, FHRS,† Yong-Mei Cha, MD, FHRS,† Komandoor Srivathsan, MD*

*From the *Mayo Clinic Arizona, Phoenix, Arizona, and †Mayo Clinic Rochester, Rochester, Minnesota.*

Introduction

The occurrence of pacemaker-related malfunction resulting from firmware updates is rare. The estimated risk of reloading of previous firmware due to incomplete update is 0.161%, loss of programmer device settings is 0.023%, and complete loss of device functionality is 0.003%, as informed by the manufacturer.[1] Recently, Abbott Medical released a software patch that updates firmware to patch cybersecurity vulnerabilities. Because to date there have been no known instances of successful hacking of a pacemaker system or instances of clinical harm, the risk associated with a firmware update must be balanced against the theoretical risk of a cybersecurity vulnerability. Here we report the occurrence of malfunctions encountered during pacemaker interrogation of 3 Abbott pacemakers associated with the version 23.1.1 Abbott firmware update. The firmware update affected programmers, wireless pacemakers, and Merlin.Net remote monitoring devices, and was designed to address cybersecurity and premature battery depletion issues.[1]

Case reports

Case 1

An 85-year-old man with pacemaker dependency because of high-grade atrioventricular block had received a dual-chamber Accent DR RF pacemaker (Abbott Laboratories, Abbott Park, IL) programmed DDDR. During routine pacemaker interrogation with the programmer (model 3650) loaded with version 23.1.1 software, the device cybersecurity update prompt appeared, and the update was initiated. During the cybersecurity update process, a 4-second pause occurred before the resumption of pacing and was associated with lightheadedness in the patient. After completion of the 5-minute cybersecurity update, an attempt to export the interrogation data failed because of an error (Figure 1). The programmer was rebooted, and the battery current on the pacemaker was noted to have increased from 11 to 27 μA, with a concomitant drop in the lower limit of battery longevity (Figure 2).

KEY TEACHING POINTS

- It is important to exercise caution when performing pacemaker interrogations after new firmware updates, especially in pacemaker-dependent patients.
- Risk versus benefit of performing a firmware update should be discussed with the patient.
- A practical strategy after release of new firmware updates may be to initiate firmware updates first in nondependent patients until the safety of firmware updates is well established.

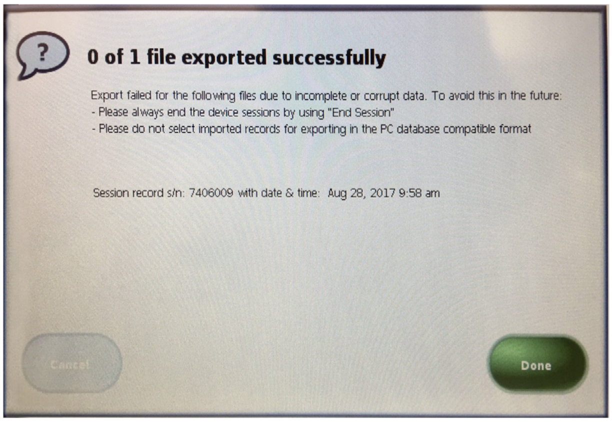
Case 2

A 74-year-old man with a history of symptomatic sinus bradycardia who had received a dual-chamber Accent DR RF pacemaker (Abbott Laboratories) programmed DDDR underwent pacemaker interrogation before magnetic resonance imaging for planned prostate cancer radiotherapy. Initial interrogation with the programmer (model 3650) loaded with version 23.1.1 software only yielded error codes (Figure 3A). Only a telemetry wand was used during the interrogation, as opposed to a wand with radiofrequency tower, and both the wand and the patient were in complete stationary positions. Another interrogation attempted with a programmer (model 3650) loaded with version 22.1.1 software permitted interrogation of the pacemaker. However, an error code appeared when programming was attempted (Figure 3B). Uninterpretable characters appeared in the patient data fields on the programming screen, suggesting malfunction (Figure 3C). Because of safety concerns, magnetic resonance imaging was canceled and rescheduled. Eventually, with the assistance of the device manufacturer engineering team, a software patch was programmed, which then permitted pacemaker programming. The patient's pacemaker was found to be programmed to DOO at 60 bpm,

KEYWORDS Cybersecurity; Firmware update; Pacemaker interrogation; Pacemaker malfunction; Pacemaker programmer malfunction
(Heart Rhythm Case Reports 2019;5:213–216)

Address reprint requests and correspondence: Dr Komandoor Srivathsan, Division of Cardiovascular Diseases, Mayo Clinic, 5777 E Mayo Blvd, Phoenix, AZ 85054. E-mail address: Srivathsan.Komandoor@mayo.edu.

https://doi.org/10.1016/j.hrcr.2018.12.013



0 of 1 file exported successfully

Export failed for the following files due to incomplete or corrupt data. To avoid this in the future:
- Please always end the device sessions by using "End Session"
- Please do not select imported records for exporting in the PC database compatible format

Session record s/n: 7406009 with date & time: Aug 28, 2017 9:58 am

Figure 1 Error message during data export attempt after firmware update. (Reproduced with permission of St. Jude Medical, ©2018. All rights reserved.)

even though the original mode was DDDR. The original settings were restored.

Case 3

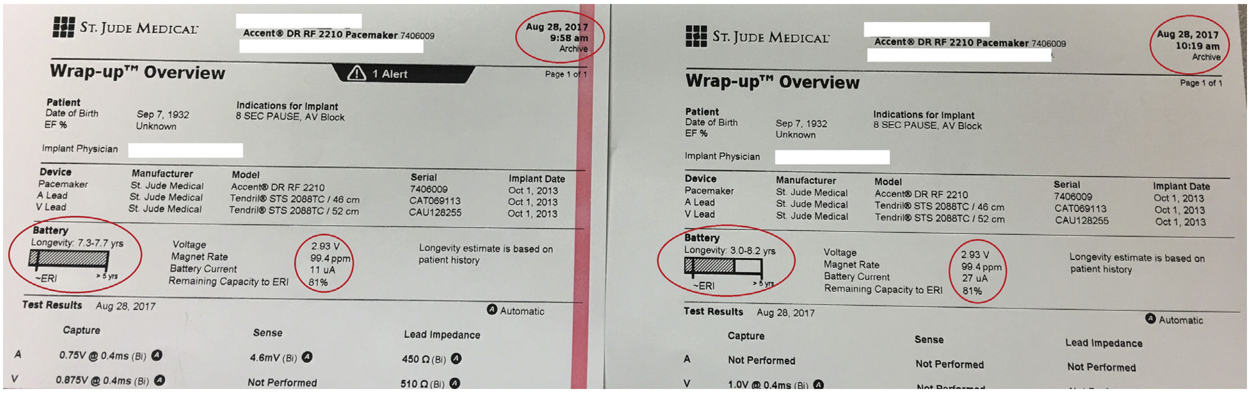
A 77-year-old man with a history of symptomatic sinus bradycardia who had received a dual-chamber Accent DR RF pacemaker (Abbott Laboratories) programmed DDDR underwent a routine pacemaker interrogation to evaluate suspected ventricular tachycardia episodes. The pacemaker had not been updated with the version 23.1.1 firmware patch. Interrogation with a programmer (model 3650) loaded with version 23.1.1 software resulted in only error codes being presented on the programmer screen. The manufacturer's engineering team provided a software patch, which ultimately permitted communication between the programmer and the device. Some garbled data had to be retyped.

Discussion

We report 3 cases of software malfunction encountered within the same week that were associated with the version 23.1.1 firmware patch update. The version 23.1.1 firmware patch update is part of Abbott's efforts to enhance cybersecurity, especially to address the risk of unauthorized programming of implantable devices. Because of online delivery to Web servers of patient physiological and device data along with near-field communication capabilities, recent cardiac implantable electronic devices (CIEDs) have increased vulnerability to cybersecurity threats.[2] Firmware is permanently embedded software programmed into ROM that provides low-level device-specific hardware control. In contrast, software provides operational instructions to applications on the device. Firmware changes are rarely performed during the lifetime of a device, whereas software updates are not infrequent. Because of CIED longevity, older operating systems that lack modern encryption are still in clinical use, potentially exposing patients to cybersecurity threats. All CIEDs at this time download device self-testing and measurements along with data on arrhythmia episodes, but programming, if needed, still requires an in-office visit.

The manufacturer states that data encryption, operating system patches, network connectivity controls, and firmware updates are all part of the recent patch designed to be delivered to the device during in-office visits. However, potential conflict between existing firmware and the current update may rarely lead to data corruption and/or device malfunction. The estimated risk of malfunction after a firmware update ranges from a 0.003% risk of loss of device functionality to a 0.023% risk of loss of programmed device settings.[1]

Our first case demonstrated a malfunction that occurred during a firmware update, during which a 4-second pause occurred. It indicates a transient loss of device pacing function that could pose a risk to patients who are pacemaker dependent. Subsequently, a change in device battery current was noted. During the firmware update, intracardiac electrograms are not available, and the device operates in a backup mode with unipolar pacing with VVI mode at 67 bpm. Given this experience, it would be important to practice caution in performing a firmware update in pacemaker-dependent patients. Our second and third cases both demonstrated that errors and corruption of data can occur when interrogating a pacemaker using version 22.1.1 software with a programmer



ST. JUDE MEDICAL [redacted]
Accent® DR RF 2210 Pacemaker 7406009 [redacted]
Aug 28, 2017
9:58 am
Archive

Wrap-up™ Overview ⚠ 1 Alert Page 1 of 1

Patient		Indications for Implant
Date of Birth	Sep 7, 1932	8 SEC PAUSE, AV Block
EF %	Unknown	

Implant Physician [redacted]

Device	Manufacturer	Model	Serial	Implant Date
Pacemaker	St. Jude Medical	Accent® DR RF 2210	7406009	Oct 1, 2013
A Lead	St. Jude Medical	Tendril® STS 2088TC / 46 cm	CAT069113	Oct 1, 2013
V Lead	St. Jude Medical	Tendril® STS 2088TC / 52 cm	CAU128255	Oct 1, 2013

Battery
Longevity: 7.3-7.7 yrs
~ERI > 5 yrs

Voltage	2.93 V
Magnet Rate	99.4 ppm
Battery Current	11 uA
Remaining Capacity to ERI	81%

Longevity estimate is based on patient history

Test Results Aug 28, 2017 Ⓐ Automatic

	Capture	Sense	Lead Impedance
A	0.75V @ 0.4ms (Bi) Ⓐ	4.6mV (Bi) Ⓐ	450 Ω (Bi) Ⓐ
V	0.875V @ 0.4ms (Bi) Ⓐ	Not Performed	510 Ω (Bi) Ⓐ

ST. JUDE MEDICAL [redacted]
Accent® DR RF 2210 Pacemaker 7406009 [redacted]
Aug 28, 2017
10:19 am
Archive

Wrap-up™ Overview Page 1 of 1

Patient		Indications for Implant
Date of Birth	Sep 7, 1932	8 SEC PAUSE, AV Block
EF %	Unknown	

Implant Physician [redacted]

Device	Manufacturer	Model	Serial	Implant Date
Pacemaker	St. Jude Medical	Accent® DR RF 2210	7406009	Oct 1, 2013
A Lead	St. Jude Medical	Tendril® STS 2088TC / 46 cm	CAT069113	Oct 1, 2013
V Lead	St. Jude Medical	Tendril® STS 2088TC / 52 cm	CAU128255	Oct 1, 2013

Battery
Longevity: 3.0-8.2 yrs
~ERI > 5 yrs

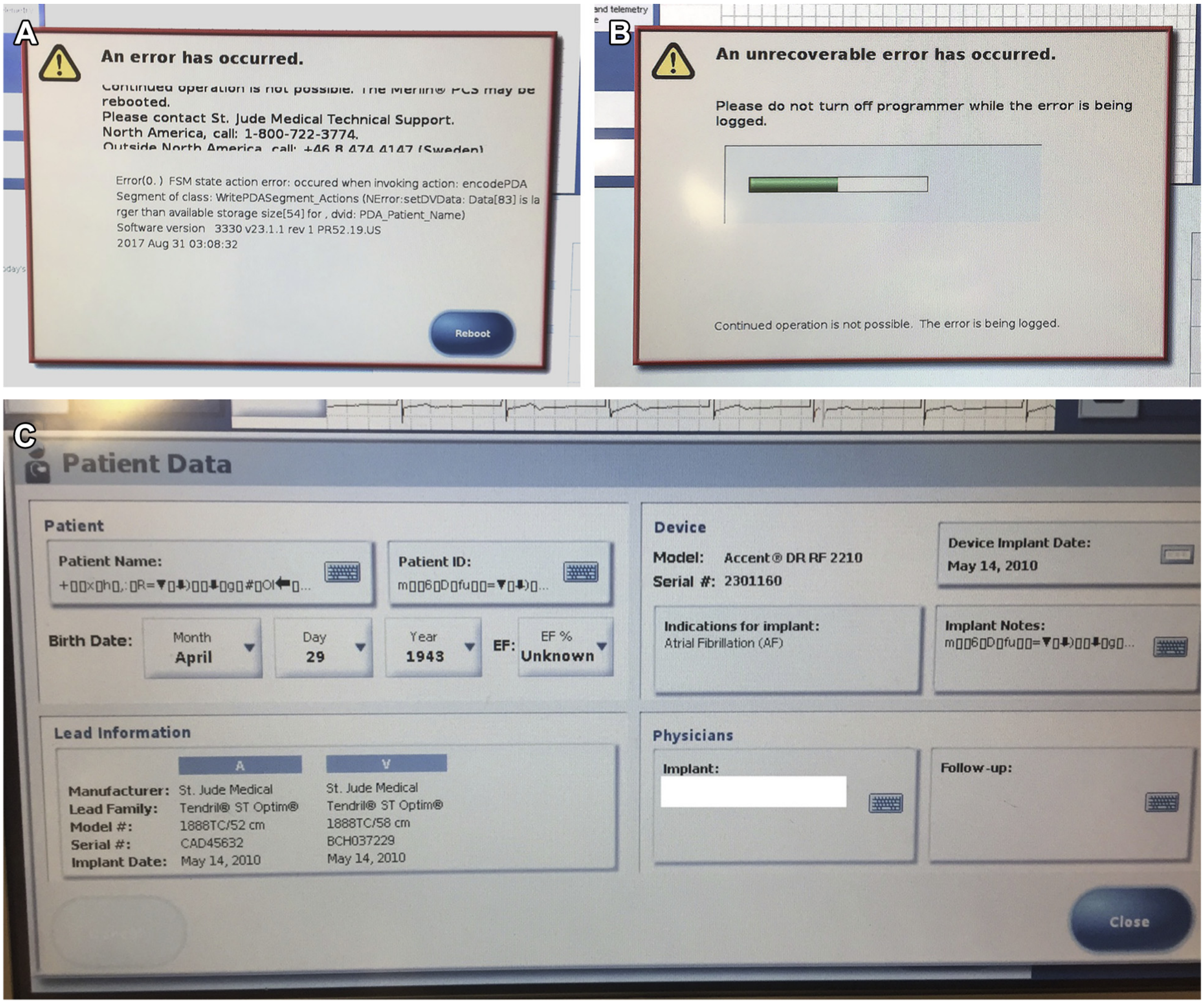
Voltage	2.93 V
Magnet Rate	99.4 ppm
Battery Current	27 uA
Remaining Capacity to ERI	81%

Longevity estimate is based on patient history

Test Results Aug 28, 2017 Ⓐ Automatic

	Capture	Sense	Lead Impedance
A	Not Performed	Not Performed	Not Performed
V	1.0V @ 0.4ms (Bi) Ⓐ	Not Performed	

Figure 2 Increase in battery current after firmware update. (Reproduced with permission of St. Jude Medical, ©2018. All rights reserved.)



An error has occurred.

Continued operation is not possible. The Merlin® PCS may be rebooted.
Please contact St. Jude Medical Technical Support.
North America, call: 1-800-722-3774.
Outside North America, call: +46 8 474 4147 (Sweden)

```
Error(0. ) FSM state action error: occured when invoking action: encodePDA
Segment of class: WritePDASegment_Actions (NError:setDVData: Data[83] is la
rger than available storage size[54] for , dvid: PDA_Patient_Name)
Software version   3330 v23.1.1 rev 1 PR52.19.US
2017 Aug 31 03:08:32
```

An unrecoverable error has occurred.

Please do not turn off programmer while the error is being logged.

Continued operation is not possible. The error is being logged.

Patient Data

Patient

Patient Name: +▯▯×▯h▯,:▯R=▼▯⬇)▯▯⬇▯g▯#▯Ol⬅▯...

Patient ID: m▯▯6▯D▯fu▯▯=▼▯⬇)▯...

Birth Date: Month April Day 29 Year 1943 **EF:** EF % Unknown

Lead Information

	A	V
Manufacturer:	St. Jude Medical	St. Jude Medical
Lead Family:	Tendril® ST Optim®	Tendril® ST Optim®
Model #:	1888TC/52 cm	1888TC/58 cm
Serial #:	CAD45632	BCH037229
Implant Date:	May 14, 2010	May 14, 2010

Device

Model: Accent® DR RF 2210
Serial #: 2301160

Device Implant Date: May 14, 2010

Indications for implant: Atrial Fibrillation (AF)

Implant Notes: m▯▯6▯D▯fu▯▯=▼▯⬇)▯▯⬇▯g▯...

Physicians

Implant: [redacted]

Follow-up:

Figure 3 **A:** Error message during initial pacemaker interrogation with version 23.1.1 programmer. **B:** Subsequent attempt with version 22.1.1 programmer permitted interrogation but not programming. **C:** Patient data were encrypted. (Reproduced with permission of St. Jude Medical, ©2018. All rights reserved.)

loaded with version 23.1.1. A potential cause of the error is disruption in the connection between the programmer and the pacemaker. In both cases, a telemetry wand was used and maintained in place at the patient's chest throughout the interrogation, suggesting that the disruption was not due to a radiofrequency communication range error. There were also no obvious environmental factors that may have led to a disruption in communication. The Accent DR RF pacemaker was involved in all 3 cases, and this may reflect potential errors when updating older pacemaker models or interrogating older pacemaker models with newer programmers.

Conclusion

This experience highlights the importance of exercising caution when performing pacemaker interrogations after new firmware updates if the programmer and implant software versions mismatch and when updating firmware, especially in pacemaker-dependent patients with older pacemaker models. A practical strategy after release of new firmware updates may be to initiate firmware updates first in nondependent patients until the safety of the firmware updates is well established. Additionally, it may be prudent to offer pacemaker-dependent patients the update in hospital surroundings where temporary transvenous pacing is readily available. In patients close to activation of the elective replacement indicator the update may be deferred altogether given that new devices are preloaded with updated software. Pre-update precautions will incorporate a full device check that includes unipolar pacing, printing or digitally storage of programmed device settings and diagnostic data in case of loss of data during update, surface leads connected with paper running, and utilization of wand alone with disconnection of radiofrequency. Most importantly, the risk vs benefit of performing a firmware update for a possible but as yet unrealized malicious cybersecurity attack should be discussed with the patient. Although software and firmware updates are unavoidable, it is reasonable to make a clinical judgment regarding the essential nature of the recommended update to determine the appropriate timing and location to perform the update. If the update is geared toward preventing a potential cybersecurity threat, most patients may not need the update immediately, especially given its attendant risks.

Acknowledgments

The authors would like to thank Julio Auto de Medeiros for his expertise and assistance with the manuscript. The authors would also like to thank St. Jude Medical for the materials used in this study, including the Tendril STS pacing lead, Accent DR pacemaker, Wrap-Up Summary Screen, and Optim lead.

References

1. U.S. Food and Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's Implantable Cardiac Pacemakers: FDA Safety Communication. Available at https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm. Accessed February 20, 2019.
2. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckl) 2015; 8:305–316.