



Muddy Waters Capital LLC
info@muddywatersresearch.com
Director of Research: Carson C. Block, Esq.

Use of Muddy Waters reports is limited by the Terms of Service on its website, which are as follows. To be authorized to access such reports, you must agree to these terms, regardless of whether you have downloaded its reports directly from the Muddy Waters Research website or someone else has supplied the report to you without authorization from Muddy Waters Capital.

By downloading from, or viewing material on the Muddy Waters Research website, you agree to the following Terms of Service. You agree that use of Muddy Waters Capital LLC's research is at your own risk. In no event will you hold Muddy Waters Capital LLC, Muddy Waters, LLC or any affiliated party liable for any direct or indirect trading losses caused by any information on this site. You further agree to do your own research and due diligence before making any investment decision with respect to securities covered herein. You represent that you have sufficient investment sophistication to critically assess the information, analysis and opinion contained herein. You further agree that you will not communicate the contents of this transcript to any other person unless that person has agreed to be bound by these same terms of service. If you download or receive this transcript as an agent for any other person, you are binding your principal to these same Terms of Service.

You should assume that as of the publication date of our reports and research, Muddy Waters Capital LLC (possibly along with or through our members, partners, affiliates, employees, and/or consultants) along with our clients and/or investors and/or their clients and/or investors, has a short position in all stocks (and/or options, swaps, and other derivatives related to the stock) and bonds covered herein, and therefore stands to realize significant gains in the event that the price of either declines. We intend to continue transacting in the securities of issuers covered on this site for an indefinite period of time, and we may be long, short, or neutral at any time regardless of our initial position and views as stated in our research.

This is not an offer to sell or a solicitation of an offer to buy any security, nor shall Muddy Waters offer, sell or buy any security to or from any person through this report or reports on the website. Muddy Waters Capital LLC is registered as an investment advisor only in the United States, but it does not render investment advice to anyone unless it has an investment adviser-client relationship evidenced in writing.

If you are in the United Kingdom, you confirm that you are accessing research and materials as or on behalf of: (a) an investment professional falling within Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); or (b) high net worth entity falling within Article 49 of the FPO.

Our research and reports express our opinions, which we have based upon generally available information, field research, inferences and deductions through our due diligence and analytical process. To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the stock covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. However, such information is presented "as is," without warranty of any kind, whether express or implied. Muddy Waters Capital LLC makes no representation, express or implied, as to the accuracy, timeliness, or completeness of any such information or with regard to the results to be obtained from its use. Further, any report on this site contains a very large measure of analysis and opinion. All expressions of opinion are subject to change without notice, and Muddy Waters Capital LLC does not undertake to update or supplement any reports or any of the information, analysis and opinion contained in them.

You agree not to distribute this information (whether the downloaded file, copies / images / reproductions, or the link to these files) in any manner other than by providing the following link: <http://www.muddywatersresearch.com/research/>. If you have obtained Muddy Waters Capital research in any manner other than by download from that link, you may not read such research without going to that link and agreeing to the Terms of Service. You further agree that any dispute arising from your viewing and use of any reports or other materials on the Muddy Waters Research website shall be governed by the laws of the State of California, without regard to any conflict of law provisions. You knowingly and independently agree to submit to the personal and exclusive jurisdiction of the superior courts located within the State of California and waive your right to any other jurisdiction or applicable law, given that Muddy Waters Capital LLC has offices in California. The failure of Muddy Waters Capital LLC to exercise or enforce any right or provision of these Terms of Service shall not constitute a waiver of this right or provision. If any provision of these Terms of Service is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision and rule that the other provisions of these Terms of Service remain in full force and effect, in particular as to this governing law and jurisdiction provision. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of this website or the material herein must be filed within one (1) year after such claim or cause of action arose or be forever barred.

Report Date: August 25, 2016	Stock Price: \$ 81.88
Company: St. Jude Medical, Inc.	Market Cap: \$23.3 billion
Ticker: STJ US	Float: 97.5%
Industry: Medical Devices	Average Volume: 1.9 million shares

This version has been updated state that Dr. Nayak speaks for himself, and not his employer.

Summary

Muddy Waters Capital is short St. Jude Medical, Inc. (STJ US).¹ There is a strong possibility that close to half of STJ’s revenue is about to disappear for approximately two years. STJ’s pacemakers, ICDs, and CRTs might – and in our view, should – be recalled and remediated. (These devices collectively were 46% of STJ’s 2015 revenue.) Based on conversations with industry experts, we estimate remediation would take at least two years. Even lacking a recall, the product safety issues we present in this report offer unnecessary health risks and should receive serious notice among hospitals, physicians and cardiac patients.

We have seen demonstrations of two types of cyber attacks against STJ implantable cardiac devices (“Cardiac Devices”): a “crash” attack that causes Cardiac Devices to malfunction – including by apparently pacing at a potentially dangerous rate; and, a battery drain attack that could be particularly harmful to device dependent users.² Despite having no background in cybersecurity, Muddy Waters has been able to replicate in-house key exploits that help to enable these attacks.

We find STJ Cardiac Devices’ vulnerabilities orders of magnitude more worrying than the medical device hacks that have been publicly discussed in the past. These attacks take less skill, can be directed randomly at any STJ Cardiac Device within a roughly 50 foot radius, theoretically can be executed on a very large scale, and most gallingly, are made possible by the hundreds of thousands of substandard home monitoring devices STJ has distributed.³ The STJ ecosystem, which consists of Cardiac Devices, STJ’s network, physician office programmers, and home monitoring devices, has significant vulnerabilities. These vulnerabilities highly likely could be exploited for numerous other types of attacks.

Key vulnerabilities can apparently be exploited by low level hackers. Incredibly, STJ has literally distributed hundreds of thousands of “keys to the castle” in the form of home monitoring units (called “Merlin@home”) that in our opinion, greatly open up the STJ ecosystem to attacks. These units are readily available on Ebay, usually for no more than \$35. Merlin@homes generally lack even the most basic forms of security, and as this report shows, can be exploited

¹ The short positions are held by funds Muddy Waters Capital LLC manages.

² See Demonstrated Attacks – Likely Just Two of Many Possibilities infra.

³ It would have been illegal to attempt to validate the large scale attack theories.

to cause implanted devices to malfunction and harm users. We believe that courts will hold STJ's lack of security in its Cardiac Device ecosystem is grossly negligent, unless STJ settles the litigation we see as inevitable.

The vulnerabilities result from an apparent lack of device security; and, the communication protocols for the Cardiac Device ecosystem – which we believe lacks basic protections such as encryption and authentication – are in fact compromised. As a result, an attacker can impersonate a Merlin@Home unit, and communicate with the Cardiac Devices – and likely even STJ's internal network. While STJ might be able to patch one particular type of attack, the mass distribution of access points to the inner workings of the ecosystem via the home monitoring devices requires in our opinion, a lengthy system rework.

Dr. Hemal Nayak, a cardio electrophysiologist at the University of Chicago, is recommending his patients unplug their Merlin@home units; and, he is not going to implant STJ devices until the problems discussed in this report are remediated. (His statement is in the Appendix.) Dr. Nayak is the medical advisor to MedSec Holdings Ltd. ("MedSec"), which is the cybersecurity research firm that identified the vulnerabilities in STJ's ecosystem.⁴ (Dr. Nayak is also a member of its board.)

Background

MedSec is a cybersecurity research firm focused on the healthcare industry. It contacted Muddy Waters after largely completing an assessment of major manufacturers' pacemakers and implantable cardioverter defibrillators ("ICDs").⁵

The lack of security in the STJ pacemaker and ICD infrastructure stunned MedSec. STJ's apparent lack of device security is egregious, and in our view, likely a product of years of neglect. Moreover, STJ's devices were even the subject of a U.S. Department of Homeland Security investigation into cybersecurity flaws in 2014, yet these gaping holes seem to persist.⁶ As a result, neither MedSec nor Muddy Waters was confident that STJ would put patients before profits if it were approached behind closed doors. Muddy Waters and MedSec agreed that users' interests are best served by being made aware of these serious issues. While standard practice in the cybersecurity industry is to notify companies of vulnerabilities before discussing them publicly, MedSec licensed its research to Muddy Waters so that we could bring these issues to light (without revealing detailed vulnerability information). Muddy Waters has engaged MedSec as consultants in addition to licensing its research on STJ. MedSec is receiving compensation related to investment profits from the funds Muddy Waters manages.

MedSec has given Muddy Waters multiple demonstrations evidencing how hollow STJ's device security is. To illustrate the severity of these vulnerabilities, MedSec demonstrated two types of

⁴ Dr. Nayak had been granted an immaterial equity interest in MedSec prior to MedSec reaching its conclusions regarding STJ.

⁵ MedSec believes this study is the first of its kind. It expects to publicly release the study in September 2016.

⁶ <http://www.reuters.com/article/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022>

attacks that could do severe harm to devices and users, and theoretically could be deployed on a large scale.⁷

In addition to making an investment case, the purpose of this report is to inform device users and their physicians of these risks. MedSec and we believe that users have a right to know that there are serious security problems with their implanted Cardiac Devices, and the related devices. However, we are withholding and redacting technical information that could give potential attackers a roadmap.

We are unaware of any imminent threat to patient safety. However, we believe it is prudent from a security standpoint for STJ to immediately disable the RF capability of patients' implanted devices. Regardless, Cardiac Device users should speak with their physicians about the risks. Muddy Waters is providing the United States Food and Drug Administration and Department of Homeland Security with a version of this report, and expects to facilitate dialogue between the agencies and MedSec.

As we detail in this report, Muddy Waters believes there is a strong possibility that STJ will need to recall its pacemakers, ICDs, and CRTs while it hardens security of the device ecosystem. This recall would likely entail a moratorium on sales of these devices, and we estimate this moratorium would be effective for a remediation period of at least two years.

The devices MedSec studied, and that formed the basis for these conclusions included pacemakers and ICDs; but, did not include CRTs. Because the CRTs are compatible with the compromised Merlin@home devices, this report assumes that they have similar vulnerabilities, and should also be recalled and remediated. (Were the CRTs not to have the expected or similar vulnerabilities, then the products would not need to be recalled.)

The Merlin@home devices were obtained second hand – often from online vendors. The programmers were obtained via a third party partnership with a licensed physician. The observations regarding device security in this report are derived from the substantial majority of devices studied, and it is possible that newer versions of these devices have some security enhancements that could eliminate some seemingly minor vulnerabilities in those particular devices.



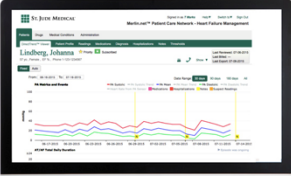

However, even if new generations of devices have some enhancements, we still view the entire ecosystem as greatly compromised. There are likely hundreds of thousands of Merlin@home devices with easily exploitable vulnerabilities in the world, and vulnerable devices are easily purchased online for no more than \$35. This train has already left the station.

STJ's Compromised Cardiac Device Ecosystem

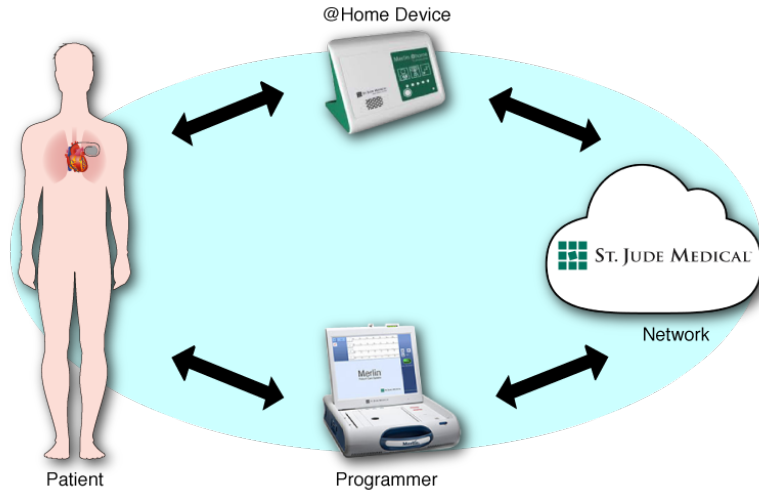
For our purposes, the Cardiac Device ecosystem consists of four components: the implantable device, the Merlin programmer, the STJ network, and the Merlin@home.⁸

⁷ It would have been illegal to try to validate the ability to commit large scale attacks.

⁸ The device pictures supra are representative, and are not pictures of the actual devices studied.

<p>Implantable Device</p> 	<p>The Cardiac Devices are implanted in patients typically to treat tachycardia and bradycardia. They are radio frequency (“RF”) enabled, so that they can communicate with the Merlin@Home devices and programmers.</p> <p>Cardiac Devices accounted for 46% of STJ’s 2015 revenue:</p> <table data-bbox="695 453 1227 520"> <tr> <td>ICDs and CRTs</td> <td>\$1,582 million</td> <td>29%</td> </tr> <tr> <td>Pacemakers</td> <td>\$941 million</td> <td>17%</td> </tr> </table>	ICDs and CRTs	\$1,582 million	29%	Pacemakers	\$941 million	17%
ICDs and CRTs	\$1,582 million	29%					
Pacemakers	\$941 million	17%					
<p>Programmer</p> 	<p>Physician office programmers (called “Patient Care Systems”) are roughly the size of a typewriter. They are critically important devices in the STJ Cardiac Device ecosystem. The programmer, typically used by a physician or medical professional, is designed to interrogate, program, display data and test STJ implantable devices. Every feature that can be changed in the implantable can be done by the programmer, as there is no other device with a higher level of sophistication. For an RF capable implantable device, a wand is used to unlock the device, and then the transmission of data occurs over RF. The programmers studied lack encryption and also present a substantial vulnerability.</p>						
<p>Merlin.net Network</p> 	<p>The STJ network enables the transfer of data between the implanted devices, programmers, Merlin@home, and physicians. Information transmitted includes patient data, remote performance diagnostics, and updates related to the device.</p>						
<p>Merlin@Home</p> 	<p>The Merlin@Home device, which is about the size of a hardcover book, communicates with Cardiac Devices over RF. Its purpose is to receive device and patient health data from the Cardiac Devices, and then transmit it to STJ’s Merlin.net network. There are literally hundreds of thousands of @home devices in the wild, and used devices with easily exploitable vulnerabilities are readily available on Ebay. The devices contain critical information and code without encryption, and are effectively “keys to the castle” that open the door to attackers.</p>						

Any programmer or Merlin@home device can generally communicate with any Cardiac Device because there is no strong authentication built into the protocol. Attackers who can reverse engineer the communication protocol can access and impersonate parts of the ecosystem, including the Cardiac Devices.



Usually, devices part of an ecosystem such as this one would have defenses including strong authentication, encrypted software and code, anti-debugging tools, and anti-tampering mechanisms. A manufacturer might also require wand activation before allowing RF communication (meaning the home device would have to be within inches of the Cardiac Device). STJ's major competitors have used the aforementioned techniques (among others) to protect their protocols. The Merlin@homes studied generally had none of these defenses.

In *Security Well Below Industry Standards* infra, we present a table comparing STJ's lack of security to the major competitors studied.

Hundreds of Thousands of Keys to the Castle

Perhaps most shocking about STJ's lack of security is that it has distributed hundreds of thousands of devices that are apparently so easily analyzed for vulnerabilities. There are numerous Merlin@home units for sale on Ebay – usually for no more than \$35. The below screenshot shows the ready availability of the Merlin@home devices on Ebay.⁹

⁹ The search was run on August 3, 2016.

ebay.com

Sign in or register | Daily Deals | Gift Cards | Sell | Help & Contact | Shop smarter | My eBay

merlin @home St jude | All Categories | Search | Advanced | Include description

Refine your search for merlin @home St jude

Categories: Health & Beauty, Other Medical Monitoring

Condition: New (3), Used (8)

Price: \$ to \$

Format: All Listings (11), Auction (0), Buy It Now (11)

Item Location: Default, Within 100 r of 95448, US Only, North America, Worldwide


Delivery Options: Free shipping


Show only: Returns accepted, Completed listings, Sold listings


More refinements...


All Listings | Auction | Buy It Now | Sort: Best Match | View: [Grid]


merlin @home St jude 11 listings | Follow this search


- 

St. Jude Medical (EX-1150) Merlin Home Transmitter
\$10.99
 Buy It Now
- 

Merlin @ Home Transmitter St Jude Medical EX1150
\$22.99
 or Best Offer
- 


St. Jude Medical EX-1150 Merlin @ Home Transmitter w/ AC Adapter & Instructions
\$20.00
 Buy It Now
- 


Merlin @ Home Transmitter Model: EX1150, ST JUDE Brand New In Open Box
\$35.00
 Buy It Now
- 


Merlin @Home Transmitter St. Jude Hospital Medical Monitor Model Ex1150
\$25.00
 Buy It Now
 Free shipping
- 

Merlin @ Home Transmitter EX1100 for Pacemaker St Jude Medical
\$32.99
 Top Rated Plus

Popular on eBay

- 

Tyco healthcare Uni-Patch
\$9.99
 Buy It Now
 Free shipping
- 

Bundle Roche CoaguChek XS
\$639.99
 Buy It Now
 Free shipping
- 

Oraquick Rapid Antibody HIV Test.
\$14.75
 Buy It Now
 Free shipping

When a patient receives a Cardiac Device implant, it is usually bundled with a Merlin@Home monitor. Previous generations of these devices were shown to be vulnerable to hacking within very close proximity.¹⁰ However, these devices had wands that needed to be within inches of the Cardiac Device in order to communicate. Merlin@home devices and implants now have additional RF capabilities, with a communications range of approximately 50 feet. They now pose a far more significant risk to user safety than before. The Merlin@home devices MedSec tested generally only required approximately 10 minutes to get access to the root directory.

¹⁰ <http://www.secure-medicine.org/public/publications/icd-study.pdf>

“Getting root” on the Merlin@home devices exposes sensitive STJ network credentials. We believe the ease of getting root shows how poor the device security is. MedSec identified three methods to get root on the @home devices.

There are numerous ways in which the Merlin@home devices violate security standards (and defy logic):

- No apparent tamper-proofing or hardware identity protection. Chip models are clearly displayed, aiding the research process for an attacker.
- Unprotected software. While patient data is encrypted, the Merlin@home device has entirely unencrypted software. Competing systems use some form of encryption to protect the proprietary applications. Extracting software from the @Home device can be done by identifying the chip, and reading the data off it. The Merlin@home’s Samsung flash memory has been publicly documented to be vulnerable.¹¹
- Lack of a layered defense. In MedSec’s opinion, the use of off-the-shelf components and the lack of anti-debugging mechanisms made the Merlin@home device significantly easier to reverse engineer and locate numerous vulnerabilities. The manufacturer left many developmental items on the devices that should not be present, such scripts that allow debugging and development mode to be turned on. All of the competitors incorporated additional security measures. Some manufacturers required short range authentication (via a wand).
- Easy availability of device firmware. MedSec was also able to obtain the @home device’s firmware in three ways:
 - Decapitating the Samsung memory chip,
 - Getting root on the @home device and simply copying the files to the USB port,
 - [Redacted.]

MedSec believes a software update was likely pushed to some of the Merlin@home devices that made them appear more secure; however, in MedSec’s opinion, this update represented a very slight change in security. This might have been STJ’s response to the 2014 issues. Merlin@home units manufactured in 2016 appear to have the same type of vulnerabilities.¹²

Getting Root Opens the Door

The first shocking thing one encounters when getting root on the Merlin@home device is unencrypted security information that takes no additional effort to access. This information includes:

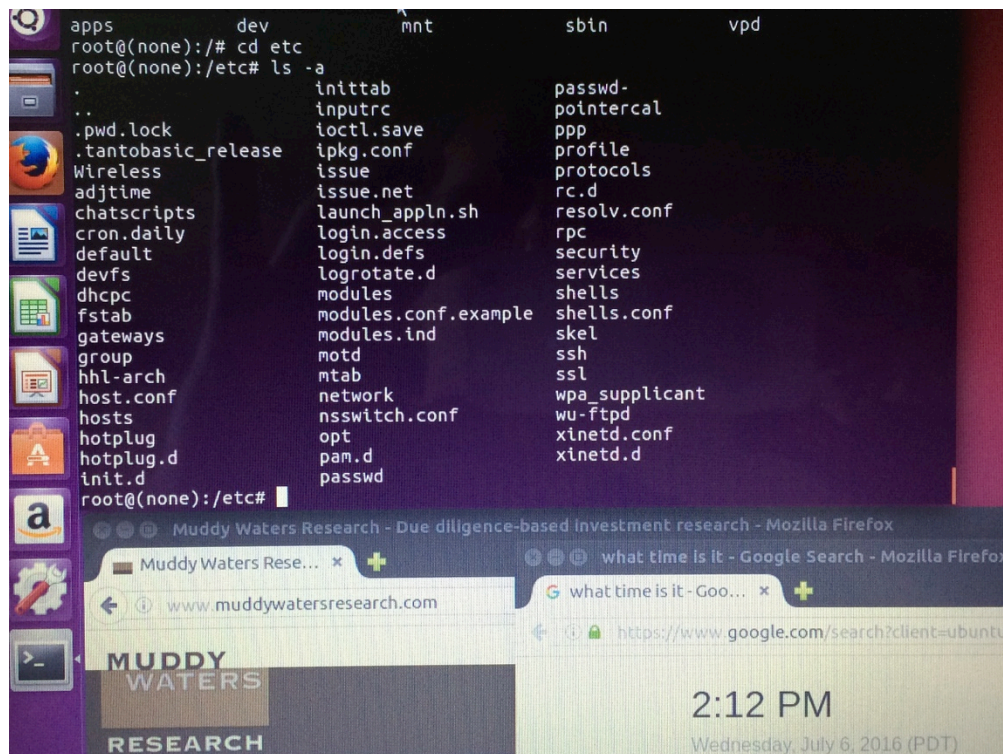
¹¹ See <https://www.blackhat.com/docs/us-14/materials/us-14-Oh-Reverse-Engineering-Flash-Memory-For-Fun-And-Benefit-WP.pdf>

¹² Devices manufactured in 2016 are difficult to obtain on the secondary market. MedSec was able to obtain one such device, and was able to get root using a previously identified exploit.

- The toll-free access number for the Merlin network. (The @home devices connect to the Merlin network either through a phone line connection or a 3G token.)
- The User ID and Password for the Merlin network. These credentials are static – i.e., they are used to authenticate all @home devices on which MedSec got root.
- STJ server IP addresses (in older device versions),
- SSH keys (in older device version). SSH keys are the “private” keys in a “public / private” key pair system. (See: https://wiki.archlinux.org/index.php/SSH_keys) MedSec is prohibited by law from testing whether these SSH keys are still in use by STJ’s network. Even if the SSH keys have been changed, their unencrypted existence on older @home devices is shocking. If the keys are still in use, they could assist an attacker with a network-based attack.

The network credentials present on the @home device likely could be exploited to obtain confidential (and legally protected) patient data from the Merlin network. Also due to legal prohibitions, MedSec was unable to confirm this theory.

Below are screenshots evidencing Muddy Waters got root on Merlin@home devices (using exploits developed by MedSec):



Security Well Below Industry Standards (the Case for Gross Negligence)

We have little doubt that STJ is about to enter a period of protracted litigation over these products. Should these trials reach verdicts, we expect the courts will hold that STJ has been

grossly negligent in its product design. (We estimate awards if litigated to a verdict could total \$6.4 billion.¹³)

One of the purposes of this report is unapologetically to single out STJ for what we see as its incompetence in, or indifference to, device security. In contrast, some competitors' devices had some surprisingly advanced device security features on home monitoring units. One competitor went as far as developing a highly proprietary embedded OS, which is quite costly and rarely seen. Healthcare cyber security is a nascent field, and one in which manufacturers and providers are challenged to catch up. However, STJ's lack of security is stunning in comparison to that of its three major competitors.

Medtronic (MDT US), the largest player in the space, took a much different approach to patient remote monitoring using the MyCareLink Patient monitor device pictured below:



MDT's MyCareLink monitor has a wand that has to be detached and put within inches of the implantable to communicate – similar to earlier versions of STJ's home monitoring devices. As a result, even if all of the MyCareLink monitors were compromised, an attacker would only be able to modify the device to perform in person attacks over a distance of a few inches.

The STJ communication protocol does not include the use of any unique or one-time tokens, such as a user-provided password. Instead, devices exchange an IMD (a unique identifier) to create sessions. As a result, any programmer or Merlin @ Home device can communicate with any Cardiac Device, and once the communication protocol is understood, **generally any device can be impersonated.**

MedSec and Muddy Waters believe it is prudent from a security standpoint for STJ to disable the RF capability of patients' implanted devices.

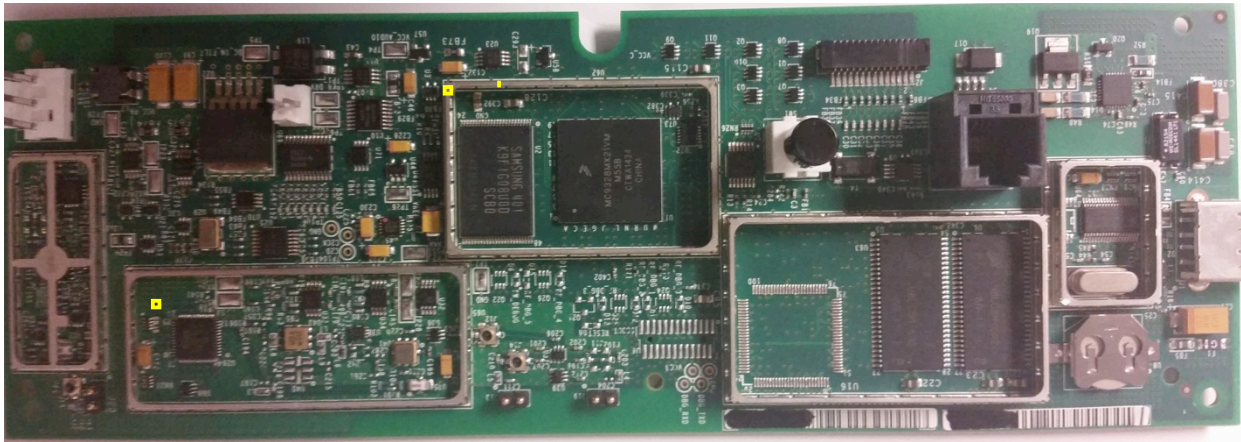
The following table compares the security on STJ's Merlin@home to the devices manufactured by the three major competitors MedSec studied.

¹³ Assumes damages of \$15,000 per each of 260,000 Merlin@home device users, plus damages of \$5,000 per each of an estimated 490,000 U.S. Cardiac Device users who do not use Merlin@home.

Vendor	STJ	Competitor 1	Competitor 2	Competitor 3
System Configuration (Encrypted?)	No	No	Yes	N/A
Application Configuration (Encrypted?)	Partial	Yes	Yes	Unknown
Core Vendor Applications (Encrypted?)	No	Yes	Yes	Unknown
Patient Data (HIPPA required) (Encrypted?)	Yes	Yes	Yes	Unknown
RF CHIP	Labeled Zarlink chip	Proprietary	Proprietary	Proprietary
Other Proprietary Chips	No	Yes	Yes	Yes
Device / Programmer communications	Vulnerable	No current vulnerabilities	No current vulnerabilities	No current vulnerabilities
SSH keys & Server IPs	In circulation on many @ home devices	Not found - Unlikely to exist on device	Not found - Unlikely to exist on device	Not found - Unlikely to exist on device
Wand Required	No	Yes	No	No
Software Hardening	Very limited, older Linux distribution	Unknown	Unknown	Unknown
Development Scripts	Left in device	Unknown	Unknown	Unknown
Update Mechanism	Vulnerable	Unknown	Unknown	Unknown

The Merlin@home circuit board shows some of the device's substandard security. STJ's RF chip is clearly an off the shelf un-customized Zarlink chip. (There is a readily available datasheet that contains important information about the packet structure the Zarlink chip uses.) In contrast, the other manufacturers have proprietary RF chips developed specifically for their protocols.¹⁴ STJ also uses a Samsung memory chipset for which there is a public presentation about how to extract the contents. Further, none of the major chips appear to be proprietary. The competitors' devices contained numerous customized chips (with no publicly available data sheets).

Samsung K9F1208 Family
Memory Chipset



Zarlink Chip

Whether SJM's conduct constitutes simple negligence, gross negligence, or recklessness we leave to the courts, based on a full discovery record. What we can say is that it constitutes an extreme departure from industry standards, as evidenced by the security efforts its competitors have made, and further shows a remarkable indifference to protecting its customers from cybersecurity threats. Regardless, we have little doubt that STJ is about to enter a period of protracted litigation over these products. Should these trials reach verdicts, we expect the courts will hold that STJ has been grossly negligent in its product design. (We estimate awards could total \$6.4 billion.¹⁵)

Merlin Programmers are also Non-Secure

Perhaps more worryingly, the physician office programmers are not well secured either. Shockingly, the STJ programmer has an easily accessible removable SATA/IDE harddrive. The hard drive is unencrypted and applications can be easily read from, modified, and rewritten to the

¹⁴ The competitors' RF chips could be custom modified chips produced by a major manufacturer such as Zarlink.

¹⁵ Assumes damages of \$15,000 per each of 260,000 Merlin@home device users, plus damages of \$5,000 per each of a conservatively estimated 490,000 U.S. Cardiac Device users who do not use Merlin@home.

hard drive using a SATA/IDE to USB adapter cable. This makes the vulnerability discovery process for an attacker significantly easier. If the applications are reverse engineered it could potentially allow an attacker emulate the full functionality of the programmer using custom hardware in a much more compact form – e.g., a pocket size device.

These devices are readily available online for a few thousand dollars – including occasionally on Ebay. A Merlin programmer available on Ebay on August 10, 2016:

The screenshot shows a web browser window displaying an eBay listing. The browser's address bar shows 'ebay.com' and the date 'Wednesday, August 10, 2016'. The listing title is 'St Jude Medical MERLIN 3650 Patient Care System w/ 3630, 3625, & Cord'. The item condition is 'Used'. The price is listed as 'US \$3,499.99'. There are '2 watching' and '30-day returns' are offered. The seller is 'omni-tech-recycling (502)' with a '100% Positive feedback' rating. The listing includes a main image of the device and a smaller thumbnail image. The shipping location is 'Troy, New York, United States' and it ships 'Worldwide'. Payment options include PayPal, Visa, Mastercard, American Express, and Discover. The listing also features a 'PayPal CREDIT' option and an 'eBay MONEY BACK GUARANTEE'.

File Edit View History Bookmarks Window Help
ebay.com
Wednesday, August 10, 2016
View as Analog
View as Digital
Open Date & Time Preferences...

Shop by category Search... All Categories
Back to search results | Listed in category: Business & Industrial > Healthcare, Lab & Life Science > Medical Equipment > Monitoring Systems > Other Med Monitoring Systems

St Jude Medical MERLIN 3650 Patient Care System w/ 3630, 3625, & Cord

Item condition: Used

Price: **US \$3,499.99**

Buy It Now

Add to cart

2 watching

Add to watch list

Add to collection

30-day returns

Located in United States

Shipping: Calculate
Item location: Troy, New York, United States
Ships to: Worldwide

Delivery: Varies

Payments: PayPal VISA MASTERCARD AMERICAN EXPRESS DISCOVER
Credit Cards processed by PayPal

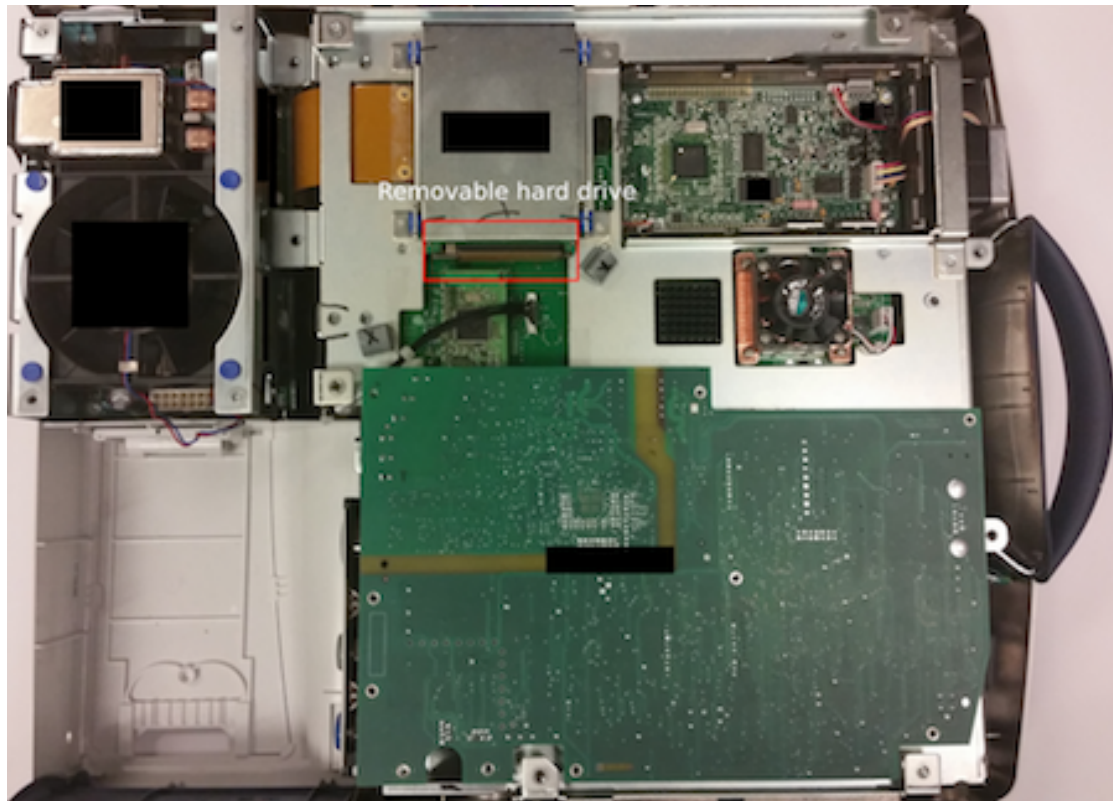
PayPal CREDIT
6 months to pay on \$99+. Apply Now | See Terms
See details

Returns: 30 days money back, buyer pays return shipping | See details

Guarantee: eBay MONEY BACK GUARANTEE | See details
Get the item you ordered or get your money back.
Covers your purchase price and original shipping.

Mouse over image to zoom

Have one to sell? Sell now



Incompetence or Indifference?

We believe the foregoing issues evidence a company that either does not know how to do device security, or does not care about it. Ironically, STJ touts its claimed strength in network security.¹⁶ It strikes us as bizarre that STJ seems so focused on its internal corporate network, which is arguably its last line of defense (and does nothing to protect against local attacks), while distributing hundreds of thousands of non-secure Merlin@home devices into the homes of its customers.

Although MedSec has spent considerable time researching STJ's devices (and those of its major competitors), it expects that there are numerous additional security issues with its Cardiac Device ecosystem. MedSec extrapolates this based on the obvious lack of attention to security evident in the devices it has researched. This seeming shoddiness is more likely than not a systemic problem at STJ, rather than an isolated one.

MedSec was able to review only a small portion of the massive code base, yet it found vulnerabilities on a regular basis. STJ should and could identify and fix these as subset of the MedSec identified vulnerabilities, and new vulnerabilities will likely continue to exist, unless

¹⁶ STJ seems quite proud of its "CTAC" – "Cyber Threat Action Center". "CTAC's mission is to identify, protect against, respond to, and enhance resiliency against cyber security threats. Learn how St. Jude Medical fulfills this mission by using threat intelligence to monitor for emerging threats against the healthcare industry and make informed verdicts on events in its SIEM." <https://www.recordedfuture.com/st-jude-medical-webinar-announcement/>

STJ reworks large portion of the code of the Merlin@home, Programmer, and implantable Cardiac Devices. The company should include anti-fuzzing, anti-debugging methods, buffer overflow protection, integer overflow protection, and string format protection.

Demonstrated Attacks – Likely Just Two of Many Possibilities

In the U.S. alone, STJ has over 260,000 active Merlin@home devices in the homes of users of Cardiac Devices.¹⁷ (The worldwide number is likely hundreds of thousands of units higher.) Many Merlin@home users keep the devices in their bedrooms, connected to STJ’s network while they sleep.

With relatively little effort, MedSec exploited tools on the @home devices to code the attacks. Then, using compromised @home devices or software defined radios (“SDR”), MedSec demonstrated two types of potentially catastrophic attacks:¹⁸

- “crash” attacks that remotely disable cardiac devices, and in some cases, appear to cause the Cardiac Device to pace at a dangerous rate, and
- a battery drain attack that remotely runs Cardiac Device batteries down.

These attacks were all demonstrated locally – within 50 feet, which is the approximate broadcast radius of a Merlin@home unit. (More powerful antennae can theoretically increase the range.) MedSec outlined an exact method that could be used to launch similar attacks on a large scale basis – either through established techniques for [redacted], or possibly through STJ’s network itself. It would have been illegal for MedSec to test the proof of concept.

It is important to note that MedSec demonstrated these attacks on pacemakers and ICDs. CRTs, which were 16% of 2015 revenue, were unavailable for the demonstrations. Because these attacks exploit the communication protocol between the Merlin@home devices and the Cardiac Devices, MedSec is confident that CRTs are similarly vulnerable.

a. “Crash Attacks”

The Crash Attacks involve broadcasting a combination of signals that places Cardiac Devices into a state of malfunction. Many of the Cardiac Devices tested are vulnerable to attacks broadcast through a single Merlin@home device that is either compromised, or via a software defined radio (“SDR”) using a broadcast antenna. The Crash Attacks generally took less than one hour to take effect.

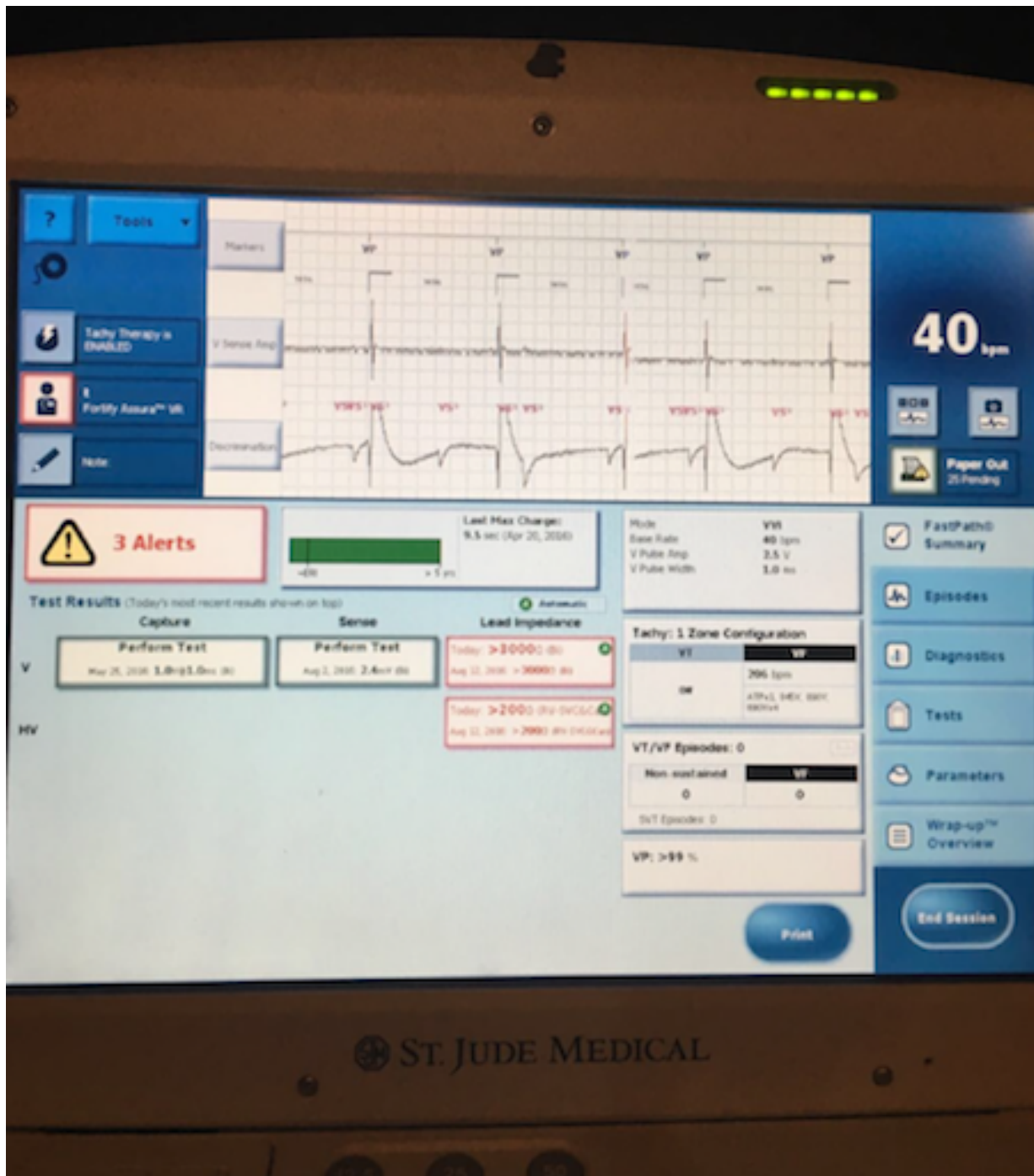
¹⁷ As of May 2014 – see <http://investors.sjm.com/investors/financial-news/news-release-details/2014/Pacemaker-and-Defibrillator-Patients-Adhering-to-Remote-Monitoring-with-St-Jude-Medicals-Merlin-Technology-Saw-More-than-Double-Survival-Rate/default.aspx>

¹⁸ “Software-defined radio (SDR) is a radio communication system where components that have been typically implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.” - https://en.wikipedia.org/wiki/Software-defined_radio (citing: Software Defined Radio: Architectures, Systems and Functions (Markus Dillinger, Kambiz Madani, Nancy Alonistioti) Page xxxiii (Wiley & Sons, 2003, ISBN 0-470-85164-3))

In many cases, the Crash Attack made the Cardiac Device completely unresponsive to interrogations from Merlin@home devices and Merlin programmers. It was therefore impossible to tell whether, and how the Cardiac Devices, are functioning. MedSec strongly suspects they were in many cases “bricked” – i.e., made to be non-functional. It is likely physicians would explant a device that did not respond to the programmer.

In some cases, a Cardiac Device subjected to a Crash Attack was still able to communicate with the programmer, and the information displayed was alarming. In a Crash Attack demonstration we witnessed on an ICD, the Crash Attack appears to have caused the device to pace at a rapid rate that could have adverse health consequences if it performed this way in a user.¹⁹ Below is a screenshot from the programmer showing the apparent malfunction. The red error messages above the lowest line are also indicators that the device is malfunctioning.

¹⁹ Interpretation of pacing data by MedSec medical advisor and board member, Dr. Hemal Nayak. See The Appendix.



b. Battery Drain Attack

MedSec has demonstrated a Battery Drain attack that generates signals from the Merlin@home device to run down batteries in Cardiac Devices at a greatly accelerated rate. The attack version MedSec tested depleted the batteries at approximately three percent of capacity per 24-hour period.²⁰ MedSec has since optimized the code. Many Merlin@home users have their devices in

²⁰ The exact depletion rate depends on the type and version of device.

their bedrooms, making it possible to run down batteries while users are sleeping.²¹ While untested, MedSec believes the new code would drain devices at six times the rate – or in approximately two weeks of nightly broadcasts. While the Battery Drain attack appears inefficient for a local attack, it could have severe consequences if deployed on a large scale.²² A minority of Cardiac Device users are device dependent, and they are the group to whom the Battery Drain attack poses the most significant risk.²³

A large scale attack is theoretically possible either through [redacted] and possibly through STJ's own Merlin network. An attack through the Merlin network could be possible because of the compromised login credentials for the network, giving rise to the possibility that the network would be unable to distinguish a genuine Merlin@home device from an attacker. Even if the particular vulnerabilities discussed in this report are fixed, the Cardiac Devices are likely susceptible to other attacks without a new communication protocol in place. Based on our conversations with industry experts, we estimate it would take at least two years to deploy a new protocol on the current generation of devices.

We are unaware of any imminent threat to patient safety. However, we believe it is prudent from a security standpoint for STJ to immediately disable the RF capability of patients' implanted devices. MedSec's medical advisor, Dr. Hemal Nayak, who is a cardiac electrophysiologist, has advised his patients to disconnect their Merlin@home units. He is no longer implanting STJ devices until the problem is remediated. (Dr. Nayak's statement to physicians and patients is in the Appendix.)

Analysis of Recall Likelihood & FDA Medical Device Cybersecurity Regulatory Framework

We believe in-home communication compatible Cardiac Devices should be recalled, either voluntarily by STJ or mandatorily by the U.S. Food and Drug Administration ("FDA"). This recall would likely take the form of a moratorium on selling new devices until STJ completes development of a new RF communication protocol. Based on our conversations with industry experts, we estimate a two-year timeline to develop and deploy the protocol.

FDA Statutory and Regulatory Basis for Device Recalls

Manufacturers independently initiate the overwhelming majority of medical device recalls.²⁴ These are labeled "voluntary" recalls conducted pursuant to 21 CFR Part 7. However, the FDA's authority pursuant to Section 518(e) of the Federal Food, Drug, and Cosmetic Act ("FDCA")²⁵

²¹ Per Dr. Hemal Nayak, MedSec medical advisor and board member.

²² Note that Cardiac Devices generally have an audible low battery indicator. A concern is that physicians and patients would assume a normal delay between onset of the indicator and depletion.

²³ http://www.medscape.com/viewarticle/712198_2

²⁴ In 2014, FDA released its "Medical Device Recall Report – FY 2003 to FY 2012" available at <http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/UCM388442.pdf> (last accessed Aug. 22, 2016). That Report states "[i]n rare cases, such as when a device firm is uncooperative, FDA may perform a mandatory recall. However, all medical device recalls during this report period were performed on a voluntary basis by the firms."

²⁵ 21 USC § 360h(e).

and its related regulations found in 21 CFR Part 810 to mandate medical device recalls likely explains the high rate of “voluntary” recalls.²⁶ Should STJ not voluntarily recall these Devices once informed of the high probability that the device would cause serious, adverse health consequences or death, the FDA has ample regulatory basis to order a recall. There are three major competing device manufacturers. While not ostensibly part of the FDA’s analysis, it is notable that recalling STJ’s Devices would not deprive patients of an essential device.

FDA Draft Guidance Document on Postmarket Device Cybersecurity

The FDA issued a draft guidance document entitled “Postmarket Management of Cybersecurity in Medical Devices” (the “Draft Guidance”) on January 22, 2016. The Draft Guidance details FDA’s current thinking on “managing postmarket cybersecurity vulnerabilities for marketed medical devices.” Specifically, the Draft Guidance provides requirements for circumstances in which cybersecurity vulnerabilities must be reported to FDA and may require additional actions, including recall.^{27,28}

The Draft Guidance focuses on “assessing the risk to the device’s essential clinical performance”.²⁹ Essential clinical performance is the “performance necessary to achieve freedom from unacceptable risk”.³⁰ Manufacturers define the essential clinical performance standards.³¹ Our analysis assumes that STJ’s definition of essential clinical performance for the Devices includes (whether explicitly or implicitly) the ability to communicate with physician programmers, avoid rapid battery depletion, and maintain safe pacing. Further, we emphasize throughout this report our view that other researchers are likely to develop additional attacks that could compromise the essential clinical performance of the Devices. The Draft Guidance acknowledges that “a cybersecurity vulnerability might impact all of the medical devices in a manufacturer’s portfolio based on how their products are developed...”³²

The Draft Guidance provides that manufacturers assess the risk a vulnerability presents to essential clinical performance by considering: a) the “exploitability” of the vulnerability, and b) the severity of the impact to patients’ health if it were exploited.³³ If a risk is “uncontrolled”,

²⁶ “The vast majority of all recalls are voluntary... Recalls are almost always voluntary, meaning initiated by a firm. A recall is deemed voluntary when the firm voluntarily removes or corrects marketed products or the FDA requests the marketed products be removed or corrected.” FDA’s openFDA, available at <https://open.fda.gov/device/enforcement/> (last accessed Aug. 22, 2016).

²⁷ FDA’s Draft Guidance Document, “Postmarket Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff,” available at <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf> (dated Jan. 22, 2016, last accessed Aug. 22, 2016).

²⁸ The draft guidance is not a final agency action and is subject to modification prior to adoption. As for all FDA guidance documents, the “draft guidance, when finalized, will represent the current thinking of the [FDA] on this topic. It does not establish any rights for any person and is not binding on the FDA or the public.” topic.

²⁹ Draft Guidance, part VI.

³⁰ Draft Guidance, part IV.E.

³¹ *Id.*

³² Draft Guidance, part V.B.

³³ Draft Guidance, part VI.

then manufacturers should remediate it.³⁴ Based on our conversations with industry experts, we estimate this remediation would take at least two years.

In terms of understanding the probability of an attack taking place, University of Michigan medical device cybersecurity research Kevin Fu pointed out that the malicious third party controls the probability distribution of an attack.³⁵

To determine whether a risk is uncontrolled, the Draft Guidance suggests that manufacturers look to cybersecurity vulnerability assessment tools to determine exploitability. It mentions one tool that could assist, called the “Common Vulnerability Scoring System”, version 3.0.^{36,37} Based on our inputs to the CVSS 3.0 model, the exploitability of the vulnerabilities for the Devices ranges from “High” to “Critical”. Further, FDA’s Draft Guidance indicates that manufacturers “should also have a process for assessing the severity impact to health, if the cybersecurity vulnerability were to be exploited.”³⁸ The Draft Guidance suggests one for such assessment to be the ANSI/AAMI/ISO 14971: 2007/©2010: *Medical Devices – Application of Risk Management to Medical Devices*.³⁹ Pursuant to this tool, a common term for assessing a qualitative severity level resulting in patient death would be “catastrophic” while, on the lower end of the severity spectrum, a common term for a severity level resulting in inconvenience or temporary discomfort would be “negligible.”⁴⁰

As shown supra, MedSec has demonstrated an attack that can cause a Device to pace at a potentially dangerous rhythm. MedSec has also demonstrated a battery drain attack, and certain Device dependent patients could experience severe health consequences if their Devices lost power and failed to function.⁴¹ Based on the Draft Guidance and its recommended tools, we therefore assess the severity of the exploit to patient health to be “catastrophic.” The below matrix from the Draft Guidance deems a vulnerability with high exploitability and catastrophic impact if exploited an uncontrolled risk.⁴²

³⁴ Draft Guidance, part VIC.

³⁵ <https://www.youtube.com/watch?v=shTj9WVhVyU&feature=youtu.be>

³⁶ Draft Guidance, part VI.A.

³⁷ The tool is available at: <https://www.first.org/cvss/calculator/3.0>

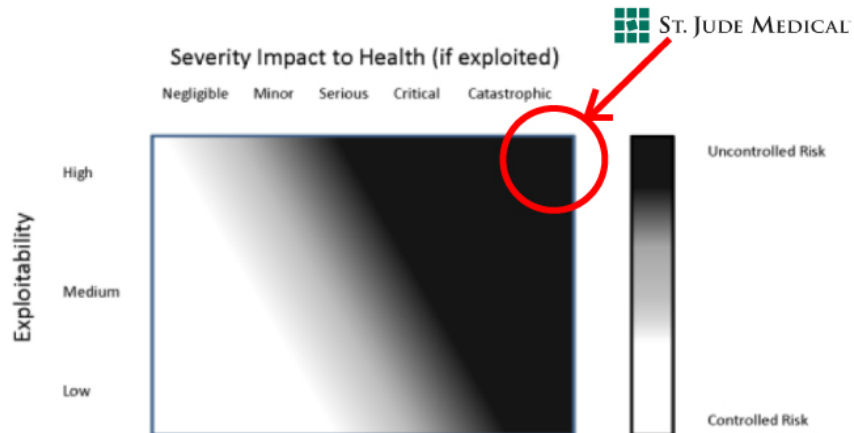
³⁸ Draft Guidance, part VI.B.

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ According to MedSec medical advisor Dr. Hemal Nayak.

⁴² The matrix is in the Draft Guidance, part VI.C.



The Draft Guidance provides several examples of uncontrolled risks. One example is strikingly similar to the vulnerabilities and attacks MedSec has discovered:

Examples of Vulnerabilities Associated with Uncontrolled Risk That Must Be Remediated and Response Actions:

A manufacturer becomes aware of a vulnerability via a researcher that its Class III medical device (e.g., implantable defibrillator, pacemaker, etc.) can be reprogrammed by an unauthorized user. If exploited, this vulnerability could result in permanent impairment, a life-threatening injury, or death. The manufacturer is not aware that the vulnerability has been exploited and determines that the vulnerability is related to a hardcoded password, and cannot be mitigated by the device’s design controls. The risk assessment concludes that the exploitability of the vulnerability is moderate and the risk to the device’s essential clinical performance is uncontrolled. The manufacturer notifies appropriate stakeholders, and distributes a validated emergency patch. The manufacturer is not a participating member of an ISAO and reports this action to the FDA under 21 CFR 806.10.⁴³

Pursuant to the Draft Guidance, FDA recommends specific changes to address vulnerabilities associated with the types of uncontrolled risks described in this example. Among other actions, the manufacturer should “identify and implement risk mitigations...such as a work-around or temporary fix.”⁴⁴ Additionally, manufacturers should report these vulnerabilities to FDA pursuant to 21 CFR part 806.⁴⁵ However, FDA states in the Draft Guidance that it does not intend to enforce these reporting requirements if three circumstances are met: 1) there are no known serious adverse events or deaths associated with the vulnerability, 2) within 30 days of learning of the vulnerability, the manufacturer identifies and implements changes to lower the

⁴³ Draft Guidance, part VII.B.

⁴⁴ *Id.*

⁴⁵ *Id.*

risk level and notifies users, and 3) the manufacturer is a participating member of an ISAO, like NH-ISAC.⁴⁶

As described in more detail *infra*, it will likely be impossible for STJ to identify and implement changes to the Devices within 30 days of learning of the vulnerabilities, and will therefore be subject to the reporting requirements imposed by FDA under 21 CFR § 806.10, which includes notification to all the customers in the distribution chain.⁴⁷

Recall Likelihood and Conclusions

The vulnerability in the ecosystem is the compromised communication protocol between the Merlin@home units and the Cardiac Devices. Because in-home units are widely available and easy to exploit, MedSec believes that STJ must develop a new communication protocol in order to secure the Cardiac Devices.

We estimate that it would take STJ at least two years to develop a new RF communication protocol. We assume the total team size required for this project would be 10 to 15 people. We understand that adding people to the team would likely not speed up the development time. Our assumption includes an expected approval timeline of three to six months.

STJ's lack of adequate attention to secure system architecture and design and implementation has resulted in an embedded system eco-system that will be very difficult to remediate. These solutions would then need to be written into the existing code base. In simpler situations, a security update can be applied to the protocol without affecting the rest of the system. In this case, STJ appears to have intertwined many of the different layers of communication throughout the software. As a result, it appears there is no part of the programming stack on which a remediation effort could focus. Large parts of the extremely large codebase would have to be re-written.

To protect existing Device users, STJ could disable the Devices' RF (radio frequency) capabilities as a "compensating control". A compensating control is a countermeasure used in the absence of sufficient controls designed into the device.⁴⁸ MedSec's observations of STJ's devices cause it to believe this is practicable to implement. With the RF disabled, devices would be unable to use the in-home devices and network and would need close proximity for interrogation. As a result, certain patients would need to see their physicians more frequently to compensate for the lack of remote monitoring.⁴⁹ It should be noted MedSec sees no reason to expect STJ's major competitors to interrupt access to their home monitoring networks.

Pursuant to 21 CFR § 7.40, STJ should recall its Devices because the Devices present "a risk of injury or gross caption or are otherwise defective" as demonstrated by MedSec's research and in light of FDA's current medical device and cybersecurity policies. Should STJ not voluntarily

⁴⁶ *Id.*

⁴⁷ FDA's "Guidance for Industry: Product Recalls, Including Removals and Corrections," *available at* <http://www.fda.gov/Safety/Recalls/IndustryGuidance/ucm129259.htm> (last accessed Aug. 22, 2016).

⁴⁸ Draft Guidance, part IV.A.

⁴⁹ According to MedSec medical advisor Dr. Hemal Nayak. However, he points out that remote monitoring improves patient outcomes and survival.

recall the Devices, FDA has a regulatory basis to and could mandate that STJ recall the Devices pursuant to its recall authority granted under section 518(e) of the FDCA and 21 CFR part 810.

Medical device recall precedents support our view that the devices should be recalled – in our opinion, the risks and severity of the STJ vulnerabilities rise at least to the levels of the following recalled devices.

Hospira Pump Recall Case Study⁵⁰

In late 2013, well-known researcher Billy Rios purchased a Hospira Symbiq infusion pump on eBay for around \$100 on a lark. Such pumps are commonplace in hospitals where health care providers use them to automatically deliver IV drips and injectable drugs to patients. Rios didn't have anything in particular in mind for the device, mostly looking to tinker. He soon discovered that he could remotely take over the device, which could have lethal consequences if used maliciously.

Recognizing the implications of his discovery, Rios sent his detailed findings to the Department of Homeland (DHS) Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In turn, ICS-CERT notified the Food and Drug Administration (FDA) and sent a report to Hospira.

Interestingly, in 2013 Hospira had already decided to discontinue the Symbiq pump and planned to spend \$300-\$350 million on doing away with its legacy pumps and developing replacements, purportedly due to scrutiny by the FDA of quality issues.^{51,52}

Months passed without Rios hearing a word from Hospira and there was no indication that government agencies were preparing to take action. Rios renewed the fight after a medical scare forced him into a hospital—and hooked up to a Hospira pump—for several days. He filmed himself hacking into the infusion pump and provided DHS and FDA with sample computer code.

This tangible evidence showing how easily he could craft code that could kill someone prompted the FDA to take action. In July 2015, it issued an advisory urging hospitals to stop using Hospira's infusion pump.^{53,54,55}

Pharmaceuticals giant Pfizer proceeded with its acquisition of Hospira (announced in February 2015) despite the negative publicity and closed the \$17 billion deal in September 2015. In May

⁵⁰ This case study draws heavily from the November 2015 Bloomberg article *It's Way Too Easy to Hack the Hospital*: <http://www.bloomberg.com/features/2015-hospital-hack/>

⁵¹ http://articles.chicagotribune.com/2013-05-02/business/ct-biz-0502-hospira-20130502_1_symbiq-infusion-device-hospira-chief-executive-f

⁵² <http://phx.corporate-ir.net/phoenix.zhtml?c=175550&p=irol-newsArticle&ID=1813491>

⁵³ <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm>

⁵⁴ <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm>

⁵⁵ <http://www.kaloramainformation.com/article/2015-08/FDA-Warning-Formalizes-Growing-Cybersecurity-Concerns-Medical-Devices>

2016, however, reports surfaced that Pfizer was looking to sell Hospira's troubled pump business for \$1.2-\$2 billion.⁵⁶

Guidant Recall Case Study

Johnson & Johnson announced that it was acquiring Guidant on December 15, 2004, for \$76 a share, at a cost of \$25.4 billion.⁵⁷ Shortly after the acquisition announcement, issues with Guidant's pacemakers and heart defibrillators arose. Almost 200,000 of its pacemakers and 88,000 heart defibrillators were impacted by safety warnings or recalls. Guidant had long failed to notify doctors of the risks of one sort of defibrillator short-circuiting.⁵⁸ The Securities and Exchange Commission opened a formal inquiry into "product disclosures and trading in Guidant stock".

Eliot Spitzer, New York's attorney general at the time, alleged that Guidant kept from the public a design flaw in one of its defibrillators.⁵⁹ Shortly afterward, Johnson & Johnson, invoked the "material adverse change" clause (MAC).^{60,61} Guidant's stock dropped to a low of \$56.53 or down 25.6% from the \$76 offer price. Ultimately, Boston Scientific stepped in and bought Guidant, but the acquisition proved to be even more costly with almost \$9 billion of write downs from 2006 to 2012 and a \$600 million settlement with Johnson & Johnson in 2015.^{62,63,64} Boston Scientific's market capitalization a few years after buying Guidant for \$27.2 billion dropped below \$13 billion and hit a low of \$7.7 billion in 2012.

Boston Scientific Case Study

Boston Scientific's ill-fated 2006 acquisition of Guidant in 2006 came to a head in March 2010 when the company announced a recall of its entire lineup of implantable defibrillators, a legacy Guidant business area. The news prompted an overnight 13% drop in Boston Scientific's share price, erased hundreds of millions in annual revenue, and resulted in a drop in total market share for defibrillators from 28% to 22%. A study at the time by McKinsey, a consulting firm, estimated that the company would lose \$5 million each day these products were off the market.^{65,66}

Boston Scientific recalled (to their credit, voluntarily) the devices upon discovering that two manufacturing process changes were made without FDA approval. The scope of those changes

⁵⁶ <http://www.biospace.com/News/pfizer-rumored-to-be-selling-its-hospira-pumps/417636>

⁵⁷ <http://www.investor.jnj.com/releasedetail.cfm?releaseid=150615>

⁵⁸ <http://www.washingtonpost.com/wp-dyn/content/article/2005/06/17/AR2005061700680.html>

⁵⁹ <http://www.wsj.com/articles/SB113103013711487375>

⁶⁰ <http://www.themiddlemarket.com/maj/20051201/31774-1.html>

⁶¹ <http://www.economist.com/node/5139360>

⁶² https://www.lawyersandsettlements.com/articles/guidant_pacemaker/guidant-pacemakers-settlement-01212.html?utm_exp=3607522-13.Y4u1ixZNSt6o8v_5N8VGVA.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F

⁶³ <http://www.wsj.com/articles/SB10001424052748704471204575210191743610672>

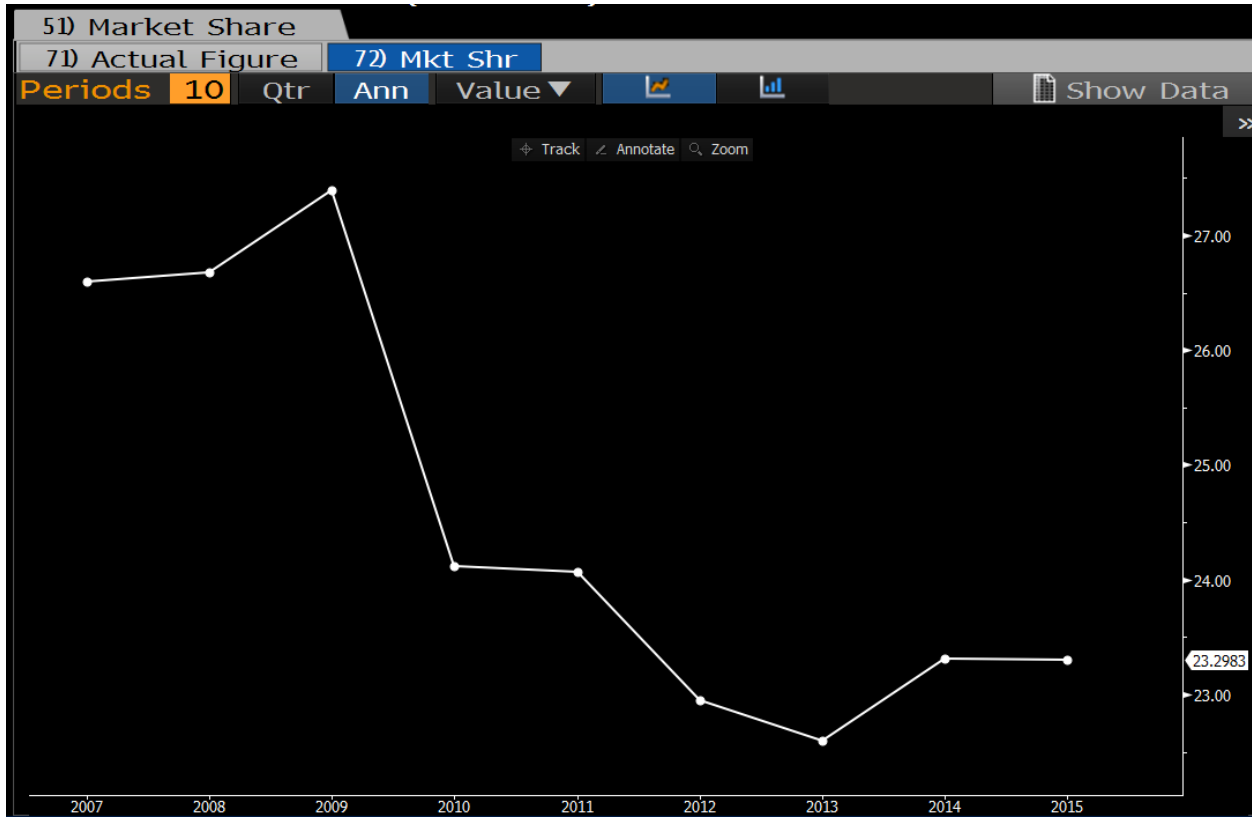
⁶⁴ <http://blogs.wsj.com/moneybeat/2015/02/18/can-boston-scientific-finally-move-on-from-its-guidant-mistake/>

⁶⁵ McKinsey and Company, *The Business Case for Medical Device Quality*, p. 4.

⁶⁶ <http://www.reuters.com/article/dealtalk-bostonscientific-idUKN0113666920100401>

was not divulged. The company asked doctors to cease implanting the devices and return all inventory, although implanted devices were deemed safe.⁶⁷

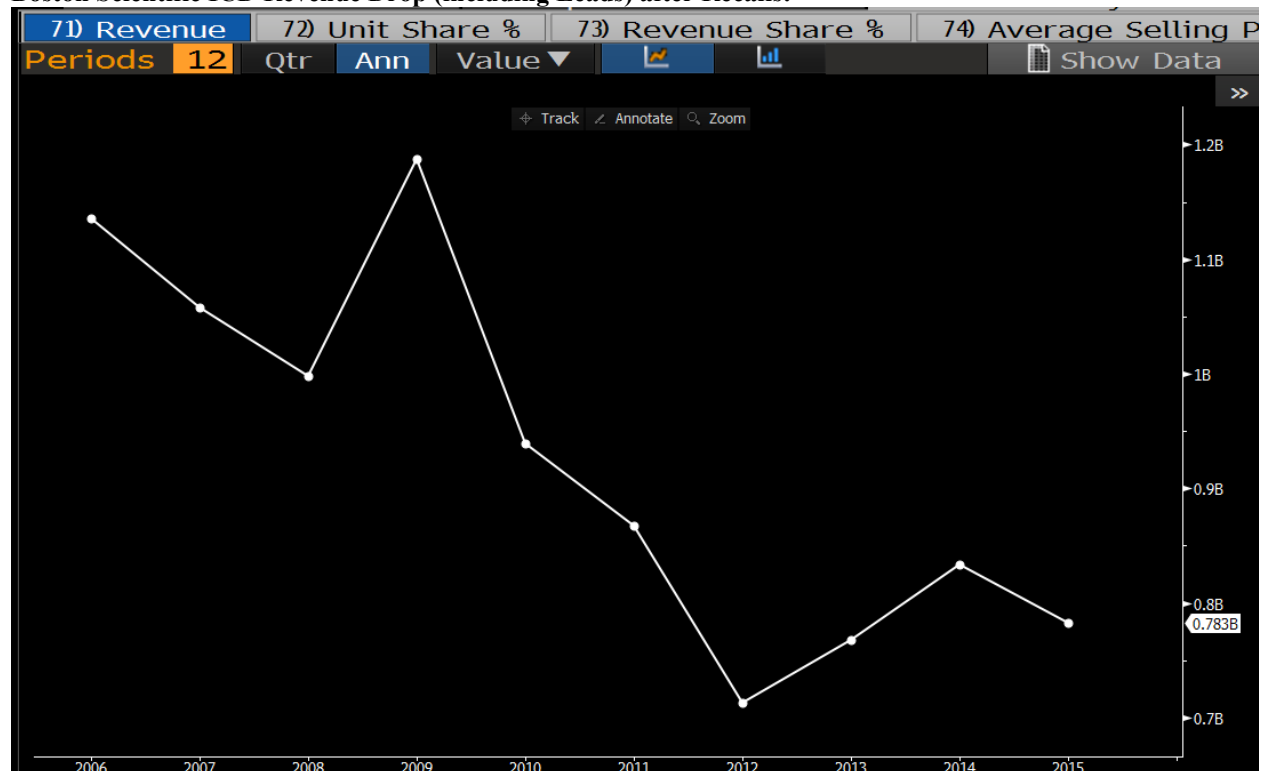
Boston Scientific Revenue Market Share Loss:



*Millennium Research Group

⁶⁷ http://www.drugrecalllawyerblog.com/2010/03/heart_devices_and_the_companie.html

Boston Scientific ICD Revenue Drop (including Leads) after Recalls:



*Millennium Research Group

Valuation

Revenue Segment	Revenues (\$MMs) % of Revenues	
	2015	
Traditional CRM (Pacemakers & ICDs)	\$ 1,617	29%
Heart Failure (78% Related to CRTs)	868	16%
Total Related to "Cardiac Devices"	\$ 2,485	45%

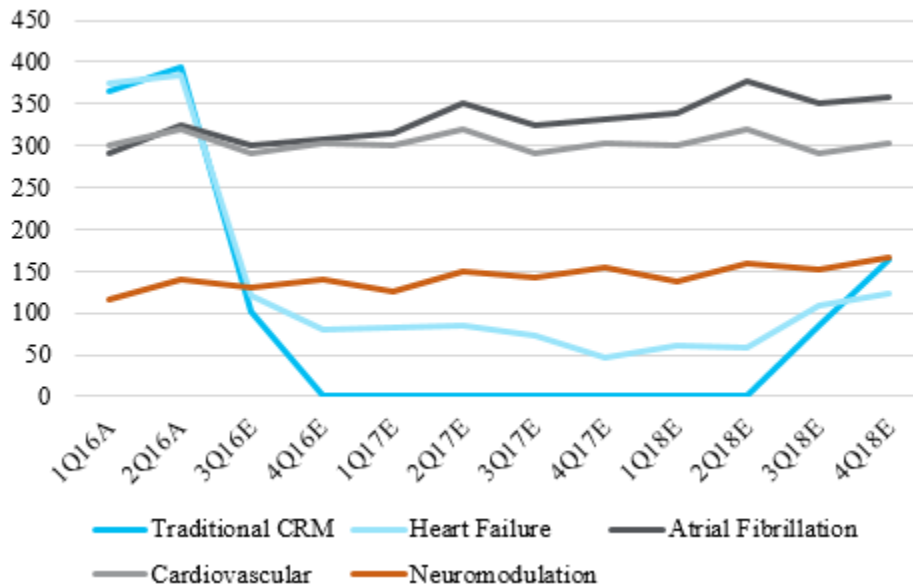
Network Shut Down and Repair Scenario:

Assumes that St. Jude shuts down the Merlin@home network for eight quarters to repair and re-architect the entire network. We think approximately 46% of St. Jude’s revenues could be related or connected to the Merlin@home device. This includes the entire CRM segment and 78% of the Heart Failure segment, or 16% of total revenues. We sensitized our Discounted Cash Flow (DCF) model with the following assumptions for eight quarters and modeled out a subsequent recovery to normalized levels thereafter. Given that this scenario is more of a topline issue, we conservatively left expenses and margins relatively unchanged from management guidance to demonstrate the negative impacts to the stock price. In a more realistic scenario, expenses, capital expenditures and interest expense could be a lot higher.

Main Assumptions:

- **Traditional CRM Segment Decline:** Traditional CRM segment (25% of 2015 Total Revenues) drops to zero for eight quarters and then starts coming back in 2018 and beyond.
- **Heart Failure Segment Decline:** Approximately 78% of the Heart Failure segment (20% of 2015 Total Revenues) comes from CRT-D and CRT-P cardiac devices, which are also connected to the Merlin@home device. We reduce all Merlin network related CRT revenues to zero and assume it goes under a network repair for eight quarters.
- **Atrial Fibrillation Segment Growth:** Management 2016 guidance is in the 10% to 11% growth range. In this scenario, the CRM network slow down also impacts the AF segment, and we assume 8% growth through 2018 in this segment.
- **Cardiovascular Segment Growth:** According to management, the Cardiovascular segment is expected to grow 1% to 3% for 2016. In this scenario, the Merlin@home issues also negatively impact this segment and thus moves growth to zero percent.
- **Neuromodulation Segment Growth:** Management 2016 guidance, is in the 7% to 9% range. We think growth moves to 5% with technology security concerns in this segment.
- **Gross Margins:** Management 2016 guidance, of 69.0% to 69.5%, however we think margins will be impacted by lower ASPs and pressure from the CRM segment and thus assume 67% gross margin until 2Q18E.
- **SG&A:** Management 2016 guidance range of 31.3% to 31.8%, however we think the percentage moves higher over an eight quarter period and closer to 33%.
- **R&D:** R&D is expected to remain in the 12.5% to 13% of sales range in our model and where management has been guiding for 2016. R&D moves to 17% for an eight quarter period to leave the expense level relatively flat with 2015's R&D spend levels.
- **Other Expenses and Interest Expenses:** Management guidance for 2016 of ~\$155 million to \$165 million, primarily driven by interest expense on our outstanding debt. Interest costs would most likely increase in a scenario where their largest revenue segment was under pressure, but for purposes of this exercise we are keeping expenses in-line with current 2016 guidance through the entire DCF modeling period.
- **Tax Rate:** For full year 2016, we continue to expect the effective tax rate to be in the range of 15.5% to 16.5%.
- **Capital Expenditures:** Capex as a percent of sales is expected to increase to 5% from a historical range of 3% to 4% for an eight quarter time period and return to historical ranges thereafter.
- **Working Capital:** Working capital remains flat at zero.
- Assumes debt maturities are refinanced in the market at the moment at the same rate.
- Longer dated revenue growth rates of 12% in 2019E and 8% in 2020E, margins, capex and tax rates recover to 2015 levels and remain relatively stable.
- Assuming no foreign currency fluctuations.

Revenues by Segment

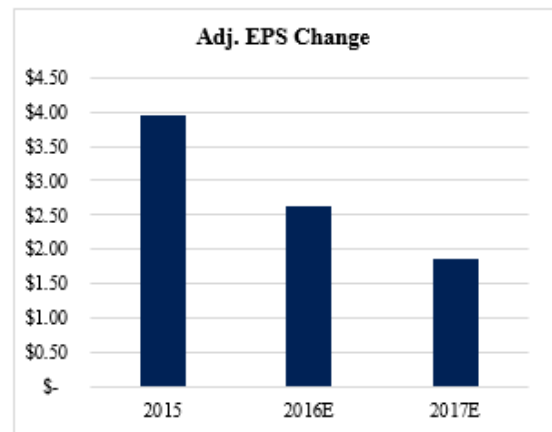


Main DCF Assumptions:

- Growth and margins return to normalized levels after eight months, for example, EBITDA margins move back to 28% in 2019, after declining to 24% in 2017.
- **WACC:** Sensitized WACC from the 6% to 11% range. According to Bloomberg, WACC was 7.7% prior to the merger announcement and peers are higher than the 6.5% currently shown on Bloomberg.
- **Perpetuity Growth Rate:** -5% to +3% growth
- **Assumes a \$1 billion settlement in four years** for product liability class actions.

DCF and Stock Price Sensitivity Results:

% of Revenues	2015	2016E	2017E	2018E
Traditional CRM	29%	18%	0%	6%
Heart Failure	20%	20%	8%	9%
Atrial Fibrillation	20%	26%	39%	37%
Cardiovascular	22%	25%	36%	31%
Neuromodulation	9%	11%	17%	16%
GAAP EPS	\$ 3.07	\$ 1.83	\$ 1.16	\$ 1.77
Adj. EPS	\$ 3.95	\$ 2.64	\$ 1.86	\$ 2.47
GAAP EPS % Change		-40%	-37%	53%
Adj. EPS % Change		-33%	-30%	33%
EBITDA % Change	4%	-19%	-35%	30%
Revenue % Change	9%	-14%	-29%	14%



Sensitivity to St. Jude Medical's current stock price is in the lower table.

		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0.0%	1.0%	2.0%	3.0%		
WACC	6.0%	8,752	9,434	10,268	11,310	12,650	14,437	16,938	20,690	26,943	Enterprise Value	
	7.0%	7,921	8,469	9,126	9,929	10,933	12,223	13,944	16,353	19,966		
	8.0%	7,224	7,670	8,198	8,831	9,604	10,572	11,815	13,473	15,794		
	9.0%	6,631	7,000	7,430	7,939	8,549	9,294	10,226	11,425	13,023		
	10.0%	6,122	6,430	6,785	7,200	7,690	8,279	8,997	9,896	11,051		
	11.0%	5,680	5,940	6,237	6,580	6,980	7,453	8,020	8,713	9,580		

		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0%	1%	2%	3%		
WACC	6.0%	7.1x	7.6x	8.3x	9.2x	10.2x	11.7x	13.7x	16.7x	21.8x	EV/EBITDA 16E	
	7.0%	6.4x	6.9x	7.4x	8.0x	8.8x	9.9x	11.3x	13.2x	16.2x		
	8.0%	5.8x	6.2x	6.6x	7.1x	7.8x	8.6x	9.6x	10.9x	12.8x		
	9.0%	5.4x	5.7x	6.0x	6.4x	6.9x	7.5x	8.3x	9.2x	10.5x		
	10.0%	5.0x	5.2x	5.5x	5.8x	6.2x	6.7x	7.3x	8.0x	8.9x		
	11.0%	4.6x	4.8x	5.0x	5.3x	5.6x	6.0x	6.5x	7.1x	7.8x		

		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0.0%	1.0%	2.0%	3.0%		
WACC	6.0%	\$ 10.61	\$ 12.98	\$ 15.87	\$ 19.48	\$ 24.13	\$ 30.33	\$ 39.00	\$ 52.02	\$ 73.71	STJ Share Price	
	7.0%	\$ 7.73	\$ 9.63	\$ 11.91	\$ 14.69	\$ 18.17	\$ 22.65	\$ 28.62	\$ 36.97	\$ 49.51		
	8.0%	\$ 5.31	\$ 6.86	\$ 8.69	\$ 10.88	\$ 13.57	\$ 16.92	\$ 21.23	\$ 26.98	\$ 35.04		
	9.0%	\$ 3.25	\$ 4.53	\$ 6.03	\$ 7.79	\$ 9.90	\$ 12.49	\$ 15.72	\$ 19.88	\$ 25.42		
	10.0%	\$ 1.49	\$ 2.56	\$ 3.79	\$ 5.23	\$ 6.93	\$ 8.97	\$ 11.46	\$ 14.58	\$ 18.59		
	11.0%	\$ (0.05)	\$ 0.86	\$ 1.89	\$ 3.08	\$ 4.46	\$ 6.10	\$ 8.07	\$ 10.48	\$ 13.48		

		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0.0%	1.0%	2.0%	3.0%		
WACC	6.0%	-87%	-84%	-81%	-76%	-71%	-63%	-53%	-37%	-11%	STJ Share Price Change*	
	7.0%	-91%	-88%	-86%	-82%	-78%	-73%	-65%	-55%	-40%		
	8.0%	-94%	-92%	-90%	-87%	-84%	-80%	-74%	-67%	-58%		
	9.0%	-96%	-95%	-93%	-91%	-88%	-85%	-81%	-76%	-69%		
	10.0%	-98%	-97%	-95%	-94%	-92%	-89%	-86%	-82%	-78%		
	11.0%	-100%	-99%	-98%	-96%	-95%	-93%	-90%	-87%	-84%		

*STJ stock price of \$82.85

Share Loss and Revenue Loss Scenario:

- In this scenario, the company loses market share and revenue, but continues to operate its Traditional CRM and Heart Failure segment. Even if the device is not recalled immediately, we think physicians and hospitals could decrease their orders of these cardiac devices given this cybersecurity issue.
- As an example, Thoratec, a heart circulatory device company that St. Jude Medical acquired in 2015, experienced severe market share loss from 2012 to 2015, after researchers published that the HeartMate II LVAD defect increased the chance of blood clots. The quarterly sales from peak to trough were down 18.4% in Q314, which was primarily driven by safety concerns with their HeartMate products. Thoratec stock dropped 30% on their 2Q14 earnings after experiencing greater than expected share loss and missing expectations.⁶⁸
- We sensitized revenues in the Traditional CRM segment to drop 14.4% in 2016E, -20% in 2017E and -8.7% in 2018E.
- The Heart Failure segment begins to decrease in 3Q16E, but grows 11.4% in 2016E and declines 20% in 2017E and begins to stabilize at -8% growth in 2018E.
- Overall revenues are flat in 2018E, +12% in 2019E and +8% in 2020E.

⁶⁸ <http://www.bloomberg.com/news/articles/2013-11-27/thoratec-s-heart-pump-may-cause-blood-clots-study-suggests>
<http://www.massdevice.com/thoratec-nejm-article-cost-us-market-share/>

- The remaining assumptions remained the same as the prior scenario.

Sensitivity to St. Jude Medical's current stock price is in the lower table.

		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0.0%	1.0%	2.0%	3.0%		
WACC	6.0%	11,811	12,720	13,831	15,220	17,006	19,387	22,721	27,721	36,055	Enterprise Value	
	7.0%	10,695	11,424	12,300	13,370	14,708	16,428	18,721	21,932	26,748		
	8.0%	9,757	10,351	11,054	11,898	12,929	14,218	15,875	18,085	21,178		
	9.0%	8,958	9,450	10,023	10,701	11,514	12,508	13,750	15,347	17,477		
	10.0%	8,272	8,682	9,156	9,709	10,362	11,146	12,104	13,302	14,842		
	11.0%	7,675	8,022	8,418	8,875	9,408	10,038	10,794	11,718	12,873		
		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0%	1%	2%	3%		
WACC	6.0%	8.3x	9.0x	9.7x	10.7x	12.0x	13.6x	16.0x	19.5x	25.4x	EV/EBITDA 16E	
	7.0%	7.5x	8.0x	8.7x	9.4x	10.4x	11.6x	13.2x	15.4x	18.8x		
	8.0%	6.9x	7.3x	7.8x	8.4x	9.1x	10.0x	11.2x	12.7x	14.9x		
	9.0%	6.3x	6.7x	7.1x	7.5x	8.1x	8.8x	9.7x	10.8x	12.3x		
	10.0%	5.8x	6.1x	6.4x	6.8x	7.3x	7.8x	8.5x	9.4x	10.4x		
	11.0%	5.4x	5.6x	5.9x	6.2x	6.6x	7.1x	7.6x	8.2x	9.1x		
		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0.0%	1.0%	2.0%	3.0%		
WACC	6.0%	\$ 21.22	\$ 24.37	\$ 28.23	\$ 33.05	\$ 39.24	\$ 47.50	\$ 59.06	\$ 76.41	\$ 105.31	STJ Share Price	
	7.0%	\$ 17.35	\$ 19.88	\$ 22.92	\$ 26.63	\$ 31.27	\$ 37.24	\$ 45.19	\$ 56.33	\$ 73.03		
	8.0%	\$ 14.09	\$ 16.16	\$ 18.60	\$ 21.52	\$ 25.10	\$ 29.57	\$ 35.32	\$ 42.98	\$ 53.71		
	9.0%	\$ 11.33	\$ 13.03	\$ 15.02	\$ 17.37	\$ 20.19	\$ 23.64	\$ 27.95	\$ 33.49	\$ 40.87		
	10.0%	\$ 8.94	\$ 10.37	\$ 12.01	\$ 13.93	\$ 16.20	\$ 18.92	\$ 22.24	\$ 26.39	\$ 31.73		
	11.0%	\$ 6.88	\$ 8.08	\$ 9.45	\$ 11.04	\$ 12.89	\$ 15.07	\$ 17.69	\$ 20.90	\$ 24.91		
		Exit Perpetual Growth Assumption										
		-5.0%	-4.0%	-3.0%	-2.0%	-1.0%	0.0%	1.0%	2.0%	3.0%		
WACC	6.0%	-74%	-71%	-66%	-60%	-53%	-43%	-29%	-8%	27%	STJ Share Price Change*	
	7.0%	-79%	-76%	-72%	-68%	-62%	-55%	-45%	-32%	-12%		
	8.0%	-83%	-80%	-78%	-74%	-70%	-64%	-57%	-48%	-35%		
	9.0%	-86%	-84%	-82%	-79%	-76%	-71%	-66%	-60%	-51%		
	10.0%	-89%	-87%	-86%	-83%	-80%	-77%	-73%	-68%	-62%		
	11.0%	-92%	-90%	-89%	-87%	-84%	-82%	-79%	-75%	-70%		

*STJ stock price of \$82.85

Covenant Breach in 3Q16 Highly Likely:

Under the network shutdown scenario, the company would breach their 4.0x bank loan covenant in 3Q16. We used Schedule 2 Section 7.13 in the Term Loan Agreement to calculate the company's Consolidated Leverage Ratio, using 2015 numbers and found that it could have already breached their covenant. Our calculation was closer to 4.45x vs. 4.25x as defined by the covenant at that time. There could have been a number of non-cash add backs that allowed it to stay current with the covenant in 2015.

SCHEDULE 2
to the Compliance Certificate
(\$ in 000s)

Section 7.13 - Consolidated Leverage Ratio

A. Consolidated EBITDA for four consecutive fiscal quarters ending on above date (“Subject Period”):	2015	Note
1. Consolidated Net Income for Subject Period:	\$	866 1
2. Consolidated Interest Charges for Subject Period:	\$	103
3. Provision for income taxes for Subject Period:	\$	62
4. Depreciation expenses for Subject Period:	\$	218
5. Amortization expenses for intangibles for Subject Period:	\$	116
6. Non-cash expenses reducing Consolidated Net Income for Subject Period:	\$	160 2
7. Non-cash items increasing Consolidated Net Income for Subject Period:	\$	87 3
8. Consolidated EBITDA (Lines I.A.1 + 2 + 3 + 4 + 5 + 6 - 7):	\$	1438
B. Consolidated Funded Indebtedness at Statement Date:	\$	6392
C. Consolidated Leverage Ratio (Line I.B ÷ Line I.A):		4.45
Covenant		4.25

Note

1 Before minority interest

2 Share compensation

3 FV adjustments for contingent consideration

The company is already close to breaching the covenant and is suffering from a slowdown in its Traditional CRM products. We think any additional pressure on the topline would cause a breach in the covenant in the near-term. As a reminder, the covenant does step down to 4.0x in 2016 from 4.25x in 2015 and then down to 3.5x thereafter. We believe the company will need to renegotiate this covenant in a timely manner and banks could ask for security (potentially \$3.8 billion of secured debt when including the revolver and term loan), higher lending rates and lower the capacity on the \$1.5 billion revolver, further straining liquidity. Any default that could arise from a covenant breach on the term loan would also be a cross default into the bonds.

Potential Liquidity Issues:

Liquidity could start becoming constrained after a covenant breach, which could lead to a reduction to its \$1.5 billion revolving credit facility and potential downgrades to their commercial paper (CP) rating, which is currently at A-2/P-2. The company is highly dependent on its CP program for liquidity and currently has \$387 million of commercial paper outstanding. Any disruption in the CP rating could negatively impact their access to this market. St. Jude Medical does have yearly debt amortization from its term loan, and its nearest bond maturity (\$500 million) is in September 2018, which could be an issue to refinance if it does not address

these issues with its Merlin network. In 2015, the company generated \$853 million of free cash flow (Cash from Operating Activities less Capital Expenditures).

Potential Credit Rating Downgrades:

Rating agencies already have St. Jude Medical on negative watch for a downgrade. The companies increasing leverage profile from its recent acquisitions has tipped leverage over 4.25x, which is already high for a single A rated company. According to a Moody's report in May 2016, Investment Grade Leverage (Debt/EBITDA) for 2015 was 2.35x vs.4.25x for STJ.⁶⁹ Along with the potential Merlin network issues, we think agencies will need to reevaluate their ratings and possibly downgrade their ratings increasing the company's borrowing costs and cost of capital.

⁶⁹ Moody's Sector In-depth Report May 20, 2016, page 10

Appendix

Letter to Patients and Physicians from MedSec medical advisor and board member Dr. Hemal Nayak⁷⁰

Dr. Nayak speaks for himself, and not his employer.



Hemal Nayak, MD, FACC, FHRS
5841 S. Maryland Avenue | MC 9024
Chicago, IL 60637

August 25, 2016

Dear Patients and Colleagues,

As a cardiac electrophysiologist, I specialize in treating patients with heart rhythm disorders particularly those that require treatment with cardiac implantable electronic devices (CIEDs) such as pacemakers and defibrillators.

I am currently an assistant professor of medicine at the University of Chicago Medicine and a board certified electrophysiologist in practice for over 15 years.

I decided to partner with MedSec because their research complements my research and interest in device function and device vulnerabilities. I serve as a consultant to MedSec and I am the principle Medical Officer in charge of medical studies as well as a board member.

Like many of my colleagues who recommend and implant CIEDs, I assumed that these devices are cybersecure. Sadly, from the research that MedSec has done, that is not uniformly the case. While I am not an expert in cybersecurity, I have witnessed, first-hand, the experiments MedSec has conducted and I have reviewed their findings.

Today, a financial partner issued a statement to the FDA based on research conducted by MedSec highlighting the cybersecurity vulnerabilities of CIEDs manufactured by St. Jude Medical. Of note, the FDA encourages all stakeholders in medical device therapy to identify, report and collaborate to reduce cybersecurity risk.

(<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf>)

In the past, popular media have sporadically reported on CIED vulnerabilities and fictional television shows have sensationalized the threat. To date, this investigation by MedSec is the largest independent investigation into the cybersecurity of CIEDs and the first to provide meaningful results.

MedSec has exposed many ways that St. Jude Medical did not adequately protect its proprietary CIED communication scheme. This potentially enables unauthorized individuals to tamper with and affect CIED function. This research utilized St. Jude Medical's Merlin home monitoring as well as the unit's RF (radiofrequency) wireless communications system. As a physician who cares for patients with CIEDs, observing these experiments and realizing that devices could be manipulated outside of usual means was quite disturbing and upsetting.

⁷⁰ Dr. Nayak has been granted an immaterial equity interest in MedSec.

While I am hopeful that the FDA will give patients and physicians guidance on what to do in light of this research, I am writing this statement to give my opinion and provide a medical perspective on what the findings mean for patients with these devices and for physicians who care for these patients.

In my mind, this CIED cybersecurity issue is first and foremost, a patient safety issue. Based on what I have seen and the results from the experiments conducted, I feel compelled to bring this issue up to the electrophysiology community at large especially since this is the first time an issue like this has come up. Additionally, I believe that patients with these CIEDs have the right to know.

First, I would like to stress that patients with implanted CIEDs manufactured by St. Jude Medical should not worry about the immediate function or performance of their devices. MedSec has not released detailed information about the vulnerabilities publically and will not do so and the details remain confidential. That being said, there may be individuals actively trying to maliciously "hack" into CIED networks.

Until the cybersecurity issues with the Merlin home monitoring network are remedied, I have recommended to my patients that they discontinue home monitoring. Unplugging the Merlin unit from the electrical outlet will effectively turn off that function. Patients can have their CIEDs checked or interrogated in person at the office or device clinic as necessary.

Unfortunately, discontinuing home monitoring does not remove all of the vulnerabilities. Because some of the threats involve the RF or wireless communication scheme (which cannot be reduced by discontinuing home monitoring) MedSec has identified temporary solutions while the larger issues are being addressed. MedSec believes that this information will be shared with St. Jude Medical. I would encourage patients to accept any corrective patches or software from the FDA or St. Jude Medical that may reduce these risks.

For patients who don't currently have CIEDs but are considering device therapy, I advise them to discuss this cybersecurity issue involving St. Jude Medical with their physician. Device therapy saves lives and a patient should not refuse recommended device therapy based on this issue alone.

MedSec has performed security assessments of CIEDs manufactured by other companies and while not perfect, has not found serious vulnerabilities. As an electrophysiologist, I have stopped implanting CIEDs manufactured by St. Jude Medical but continue to use other companies.

For most of us, the topic of CIED cybersecurity is something "out of left field". As such, it is scary and unsettling. MedSec is working diligently and is confident that solutions to these vulnerabilities will be found and risks to patients mitigated.

Respectfully,



Hemai Nayak, MD, FACC, FHRS
Cardiac Electrophysiology