Taxonomy of Current Medical Devices for POCT Applications and the Potential Acceptance of Bluetooth Technology for Secure Interoperable Applications

Dalimar Velez and Michael Shanblatt
Department of Electrical and Computer Engineering
Michigan State University
velezdal@msu.edu, mas@msu.edu

Abstract— **This paper presents a taxonomy for medical devices that includes the review of over 260 companies. The taxonomy classifies medical device products with respect to their output interface. Each medical device in the study is portable, designed for the point of care environment, non-implantable, and includes at least one output interface. The main motivation for this study is the possible resolution of current trends in medical device interfaces designed for point of care testing (POCT) scenarios. This paper also presents the Bluetooth Health Device Profile (HDP) as a possible option for current/new designs for POCT networks that use a smart phone as the main computational and communication engine. Vulnerabilities and countermeasures for current Bluetooth technology are described. The paper concludes by proposing a transitional solution involving the utilization of an interface box that supports the current legacy medical devices.**

Keywords – Point of care testing (POCT) devices; Home health care; Bluetooth; Security; Health device profile (HDP)

I. INTRODUCTION

Point of care testing (POCT) involves the use of portable electronic medical devices to perform a variety of tests to monitor the health of a patient. These devices can be used with patients in the hospital with the growing trend towards use in home health care. Some of the functions that can be monitored by portable devices include the simple measurements of temperature, weight, peak expiratory flow rate (PEFR), blood pressure (BP), blood sugar, blood oxygen, and the more complex measurements like electrocardiography (ECG) and, to a growing extent, blood chemistry. Most POCT devices are designed for the management of chronic diseases. During the past several years, the rapid increase of home health care services and monitoring devices has brought much attention to the merger of POCT and telemedicine [1-8].

The results described in this paper are only part of a greater project that envisions the use of a smart phone as a POCT platform for home health telemedicine. In order to fulfill the goals of this research, a study to classify and categorize the medical devices on the market is foundational. Section II of this paper provides some introductory details on POCT devices. Section III presents a taxonomy of medical devices basing the comparison on their output interface and the embedded security measures. The taxonomy reveals the output interfaces most widely used in these devices, the trend in the current market, and other important details that could help the adoption process of medical standards. Section IV, "Bluetooth and Security" provides basic Bluetooth technology information along with new details on improvement of the core specifications. Furthermore, Section IV presents an overview of the Bluetooth standard, Bluetooth Health Device Profile (HDP), and Bluetooth security. This section proposes a POCT use case using an interface box that supports HDP and IEEE 11073 to maintain compatibility with legacy medical devices. Finally, conclusions are presented in Section V.

II. POCT BACKGROUND

Most of the current POCT devices are not capable of working with sensors other than the ones offered by the manufacturer. A patient with multiple and different monitoring requirements may need to utilize multiple POCT devices that share many similar functions; an approach that is obviously neither cost-effective nor efficient for the patient. It is feasible to incorporate multiple sensors in a single POCT. The concept of a POCT with multiple sensors is not a new idea. Some existing POCT devices may work with a subset of sensors, but concerns arise because there is no uniform approach available among the existing sensors to communicate with a generic POCT device. The incorporation of the health standards in the next generation of POCT is vital for compatibility and interoperability. Current developments in mobile technology create an opportunity for designing a generic application with greater advantages in size, power, and bandwidth, thus enabling the use of the device from almost anywhere.

A generic POCT scenario involving the use of a smart phone as the platform and the implementation of the IEEE 11073 standard is presented as the basis for the taxonomy of this paper. Figure 1 shows the system overview. The system consists of a personal area network (PAN) formed by the patient's POCT devices. The PAN communicates with the smart phone acting as the IEEE 11073 manager. An IEEE 11073 manager device refers to all devices that receive information from an agent device as defined in [2]. The IEEE 11073 agent devices represent any device that captures information about the patient. The smart phone creates a wide area network (WAN) to form a link to the health care provider, hospital data center or the health record system. The system manages and maintains a secure communication between the POCT, the smart phone and any remote storage center. The system has two wireless communication links that permit the transfer of the patient's data. Currently, not all the POCT devices provide wireless communication. These devices will need an interface that incorporates

wireless communication due the current limitations on available interfaces. The proposed interface box is described in Section IV. Current smart phones have a USB port whose only role is to be a slave USB device. The second communication link is the transmission from the smart phone to the health provider or data center. Both communication links require secure and reliable transmission of the information and data.

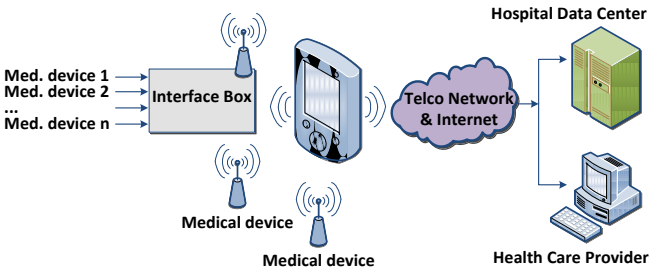

Figure 1. System overview.

With current and emerging technology, a POCT device is capable of taking a patient's vital signs, recording and/or transmitting them to a clinical system where health professionals review the patient's data. The design objectives for POCT in-home care environments are quite different from their clinical counterparts. The home care POCT needs to be easy to use, reliable, secure, fault-tolerant, and self-calibrating. Moreover, it must be capable of encrypted communication with the health care provider to insure compliance with standards protecting patient confidentiality. A majority of the POCT devices marketed (the current commercial POCT devices) have proprietary designs using various communication protocols and are isolated products lacking in interoperability [1]. This problem led many organizations to move toward the goal of establishing standardization.

The ISO and IEEE organizations worked to develop the IEEE 11073 for health informatics [2-4]. The Continua Health Alliance is working to establish and produce interoperable solutions for personal health care and to write guidelines that are based on already proven standards [5]. This alliance is taking the lead in resolving and implementing standards for health care and telemedicine [5].

The telemedicine field is under constant change and development. Each day health providers become more aware of the benefits of using technology to manage patient information. Other developments to improve interoperability in telemedicine applications are the USB Personal Healthcare Device Class (PHDC) [6], the Bluetooth Health Device Profile (HDP) [7, 11], and the ZigBee Health Care [8] public application profile.

III. TAXONOMY OF MEDICAL DEVICES

A. Selection of medical devices

The taxonomy presented in this paper classifies the medical devices with their available output interfaces. In order to produce this taxonomy, over 260 companys' current medical devices were reviewed. The initial list sourced companies used in previous market research studies [21], the web, and other advertising material available through retail distributors. Among this group of companies, all members of the Continua Health Alliance were included [5]. All medical devices considered in the study met the following requirements: portable, point of care (POC) designed, non-implantable, and with at least one output interface. The portability of the device allows the patient to have a higher degree of freedom with respect to his/her mobility while using the medical device. This means that the medical device needs to be designed to minimize the size, weight, and power requirements. Finally, the taxonomy includes only permanently non-implanted medical devices. This includes medical devices that are noninvasive or invasive for short term use only.

The output interfaces found on the medical devices include: Bluetooth, Universal Serial Bus (USB), Serial (RS232), plain old telephone service (POTS), Ethernet, IEEE 802.11, global system for mobile communications (GSM/GRS), and Infrared Data Association (IRDA). A total of 245 medical devices passed the requirements previously established. Table I shows the top 15 companies ordered by the number of medical device products that they currently produce. Table II presents the percentage of the output interfaces from all the medical devices in the list.

TABLE I. TOP 15 MEDICAL DEVICES PRODUCERS.

Company name	Medical device products
TaiDoc Technology Corporation	33
LifeWatch AG	17
Philips	11
Nonin	11
Polar	10
CareFusion	8
Braemar, Inc.	7
Abbot Lab	7
A&D Medical	7
Omron Corporation	6
Welch Allyn	6
Innomed Medical Zrt	6
Microlife Corporation	6
SHL Telemedicine	6
Vitaphone GmbH	6

TABLE II. NUMBER AND PERCENTAGE OF MEDICAL DEVICES CHARACTERIZED BY OUTPUT NTERFACE TYPE.

Output interface	Number of medical devices	Total share* %
Serial port (RS232)	85	35%
USB	71	29%
Bluetooth	59	24%
POTS	29	12%
IRDA	24	10%
IEEE 802.11	20	8%
GSMA/CDMA	16	7%
Ethernet	9	4%
RF-Wireless	8	3%

*Note that sum exceeds 100% since some devices have multiple outputs.

B. Medical devices compatible with IEEE 11073

Only 10 medical devices out of the 245 devices in the study were found to be compatible with the IEEE 11073 standard and the Continua Health Alliance. This indicates that less than the 4% of the medical devices available are interoperable. This statistic marks the beginning of the acceptance of the standards by some companies. In addition, this proves that the problem of interoperability still exists for the majority. Table III shows the 10 Continua approved products. As can be seen, the two predominant types of medical devices in this group are the blood pressure monitor (BPM) and the pulse oximeter device.

TABLE III. CURRENT CONTINUA ALLIANCE APPROVED PRODUCTS.

Company name	Type of medical devices	Product description
Omron Corporation	Pedometer	HJ-721IT Pedometer
	Body composition monitor	HBF-206IT Body Composition Monitor
	BPM - Blood Pressure Monitor	BP792IT Blood Pressure Monitor
A&D Medical	Weight scale	UC-321PBT-C Weight Scale
	BPM - Blood Pressure Monitor	UA-767PBT-C Blood Pressure Monitor
Nonin	SpO2 - Pulse oximeter	2500 PalmSAT® Pulse Oximeter
	SpO2 - Pulse oximeter	Onyx® II Model 9560 Fingertip Pulse Oximeter
Panasonic	PC	TOUGHBOOK® H1
Cambridge Consultants Ltd	BPM - Blood Pressure Monitor	Vena – BPM
	Inhaler	Vena – Inhaler

C. Medical device by type

After organizing by operation, each device was categorized by their best fit into the IEEE 11073 defined types (IEEE 11073-10101 nomenclature) [4]. The database used for the taxonomy includes a total of 39 types of medical devices. Table IV shows the top 10 medical device types found with their total number of products. These 10 types of medical devices represent approximately 67% of all the medical devices in the study and also represent the medical device types with the largest presence in the market.

TABLE IV. THE TOP 10 MEDICAL DEVICES TYPES BY TOTAL NUMBER OF PRODUCTS FOUND.

Type of medical devices	Total number of products
Glucose meter	31
BPM - Blood pressure monitor	26
System-multifunctional	20
ECG – Electrocardiography	17
SpO2 - Pulse oximeter	17
Patient monitor	14
Spirometer	11
Fitness monitors	10
Insulin pump	10
Weight scale	8

D. Output interface statistics

Table V shows the percentage of each output interface using the medical devices types from Table IV. The highlighted cells denote the top 3 interfaces (higher %) by each type of medical device. The system multifunctional type that appears on the table defines all devices that implement more than one function simultaneously and that are intended for home care use. As can be verified from Table II, the serial (RS232) interface is the most used interface, with 61% of glucose meter devices using it. This is expected due the fact that the glucose meter and serial interface are both an older medical device and interface protocol, respectively. On the other hand, it is important to point out that the serial port is not easily scalable, nor prepared to support all the features mentioned on the previous subsection conducive to a POCT scenario. It is still used because it maintains backward compatibility with legacy systems. Newer generations of medical devices should use the other two interfaces (Bluetooth or USB) to take advantage of their data throughput which is flexible enough for current and near-term future medical devices data requirements.

The most important aspect of Table V is that the Bluetooth technology appears as one of the top 3 for 8 of the 10 categories shown, and USB follows it by being in the top 3 in 6 out of 10 categories. This suggests that Bluetooth is on the path to become the preferred output interface for next generation medical devices. But for the next several years both interfaces, USB and Bluetooth, should show an increase in the number of medical device that use them as a preferred output interface.

E. Security enabled medical devices

Security measures were studied in those medical devices that include Bluetooth technology given the limitation explained in Section II. Bluetooth technology is available in most of the current smart phones. This technology also implements various mechanisms of security to protect the user and any private data transmitted. Recent developments like the Health Device Profile (HDP) provide interoperable functionality and compatibility with the IEEE 11073 standard. The HDP is a Bluetooth profile that defines the wireless connection protocol for medical devices.

Security on Bluetooth devices cannot be guaranteed without knowing some information regarding the Bluetooth specification version implemented, the encryption strength used, and profiles supported. Table VI shows the available Bluetooth devices that implement Health Device Profile (HDP) along with their Bluetooth version, the encryption strength, and any other security measure taken. Only 8 medical devices (3%) were found compatible with the HDP profile. This is a clear indication of the current state of the medical devices on the market with respect to interoperability of the devices. The next section will present more details regarding the security available in Bluetooth.

TABLE V. THE TOP 10 MEDICAL DEVICES TYPES BY THE PERCENTAGE OF THE OUTPUT INTERFACE TYPE.

Type of medical devices	RF Wireless	GSM/GPRS/ CDMA	Bluetooth	RS232	USB	IRDA	Wired Ethernet	POTS	IEEE 802.11
Glucose meter	0%	0%	13%	61%	42%	10%	0%	0%	0%
Blood pressure monitor	4%	0%	38%	35%	35%	0%	0%	4%	4%
System-multifunctional	0%	35%	30%	15%	35%	0%	10%	25%	25%
Electrocardiography	0%	35%	41%	29%	6%	0%	0%	47%	6%
SpO2 - pulse oximeter	0%	0%	35%	35%	24%	0%	0%	0%	6%
Patient monitor	0%	0%	7%	21%	29%	0%	36%	0%	43%
Spirometer	0%	0%	27%	55%	73%	9%	0%	0%	0%
Fitness monitor	0%	0%	0%	0%	0%	100%	0%	0%	0%
Insulin pump	40%	0%	30%	10%	20%	50%	0%	0%	0%
Weight scale	13%	0%	50%	13%	0%	0%	0%	13%	13%

TABLE VI. MEDICAL DEVICES THAT SUPPORT BLUETOOTH HDP.

Company name	Products description	Bluetooth version	Security
Omron Corporation	HJ-721IT Pedometer with Bluetooth docking station	v2.1 + EDR class 2	Automatically choose from HDP or SPP
	BP792IT Blood Pressure Monitor	v2.1 + EDR class 2	
	HBF-206IT Body Composition Monitor	v2.1 + EDR class 2	
A&D Medical	UC-321PBT-C Weight Scale	v2.1 class 1 HDP	128 bit encryption of data
	UA-767PBT-C Blood Pressure Monitor	v2.1 class 1 HDP	
Nonin	Onyx® II Model 9560 Fingertip Pulse Oximeter	v2.0	Data encryption and designed to meet the requirements of HDP
Cambridge Consultants Ltd	Vena	v2.1 + EDR, HDP	N/A

IV. BLUETOOTH AND SECURITY

Bluetooth is a short-range wireless communication standard that enables the establishment of wireless personal area networks (WPAN) [10]. The Bluetooth standard operates in the unlicensed Industrial, Scientific, and Medical (ISM) frequency band from 2.4000 GHz to 2.4835 GHz. Bluetooth utilizes frequency hopping spread spectrum (FHSS) to reduce interference problems and to improve security. Interference problems are caused mainly by other technologies that work simultaneously in the ISM band. These include IEEE 802.11/Wi-Fi devices, microwave ovens, and cordless telephones. Using FHSS, the Bluetooth protocol divides the band into 79 different channels. The frequency hopping rate occurs at 1600 hops/s and consequently each channel is used for 625 µs. Bluetooth v1.2 or later includes adaptive frequency hopping (AFH) to identify frequencies that are used by interference sources and avoids them in the hopping sequences [10]. This technology makes it difficult for an adversary to monitor or disturb the transmission.

Bluetooth devices are classified according to range and RF power level into 3 classes. Class 1 operates at 100 mW with a range of 100 m, class 2 at 2.5 mW with a range of 10 m, and class 3 (low power devices) at 1 mW with a range of 1 m.

The Bluetooth architecture permits the creation of ad hoc networks called piconets. A piconet consists of one master device and up to 7 slave devices. The core specification of the Bluetooth technology has 4 versions. Bluetooth versions 1.1 and 1.2 support a transmission rate up to 1 Mbps. Bluetooth version 2.0 and 2.1 have an Enhanced Data Rate (EDR) allowing data rates up to 3 Mbps [12]. Bluetooth v3.0 + High Speed (HS) specification permits a maximum throughput of 24 Mbps [13]. The latest version, 4.0, was published on June 2010. This version includes some security and Low Energy (LE) improvements [14].

The Bluetooth Special Interest Group (SIG) developed the Health Device Profile (HDP) for the specific purpose of transmitting medical data [7,11]. The medical data structure is not defined by the HDP. The HDP mandates the use of IEEE 11073-2060 [2], which defines the data exchange protocol, and the IEEE 11073-104xx [3], which is the device specialization defining the data format. This application profile allows multiple source devices (IEEE 11073 agent) to exchange data to sink devices (IEEE 11073 manager). The HDP profile is specialized for health care applications providing interoperability and standardization. Some of the specs in the HDP are the Multi-Channel Adaptation Protocol (MCAP), for reliable streaming data channels, mandatory authentication and encryption, enhanced retransmission mode in the L2CAP layer, clock synchronization protocol (CSP), reliable reconnection, and connectivity to multiple devices [11].

A. *Bluetooth security*

The Bluetooth standard offers security services as authentication, authorization, and encryption. The specification defines four security modes. The first three security modes are for Bluetooth devices that do not support Secure Simple Pairing (SSP). Security mode 1 establishes no security measures, security mode 2 provides security after the link setup (the Bluetooth security services are set for the security requirements of an application), and security mode 3 provides security at the link level before any channels are established [15]. Security mode 4 is mandatory for SSP devices and provides security after the link is established. The SSP, a new feature in v2.1 + EDR and later versions, simplifies the paring and improves the security by adding a link key generation and key exchange using a public key cryptography [14]. The two security goals of this paring process are to protect the device from passive eavesdropping and to prevent "man-in-the-middle" (MITM) attacks. SPP employs Elliptic Curve Diffie Hellman (ECDH) [12] as the public key cryptography and works on four association models depending on the I/O capabilities of the devices. The association models include [14]:

- Numeric Comparison – both devices are capable of displaying a 6 digit number and responding with a yes or no to confirm pairing if the numbers are identical.
- Passkey Entry – one device has the display capability and the other device is only capable of entering key entries. The device with the display will show a 6 digit number and the user of the other device is required to type the numbers to complete the pairing.
- Just Works – at least one of the devices has neither a display to show the 6 digit number nor a way to enter the user response. The user is asked to accept the connection without verifying the number.
- Out of Band (OOB) – one device supports OOB mechanism to discover the devices and to exchange the parameters required in the pairing process. An example is the Near Field Communication (NFC).

B. *Vulnerabilities and countermeasures*

Bluetooth technology security has been improving since its inception. However, the majority of current Bluetooth devices and those available for sale are compatible with the version 2.1 + EDR and earlier. Many of the higher risk weaknesses found in these versions permit attacks on these devices [15-19]. In some situations, these vulnerabilities are caused by the specific implementation. In other situations, problems have a risen from weaknesses found in particular version specifications of the technology.

Recent improvements to the Bluetooth specifications provide new features that make this technology a promising option for future POCT implementations [13-14]. Still, more improvements need to be made to overcome the current limitations in Bluetooth security, and possible threats that arise in different scenarios. Bluetooth technology is not exempt from the general weaknesses found in other wireless technologies which include MITM and eavesdropping. Most of these threats can occur on devices and piconets that make improper use of the Bluetooth implementation and its security features, but they also occur as a result of current security limitations in the standard [20].

Other threats have been found and new name conventions have been formed to describe the particular occurrence in the Bluetooth technology. Interestingly, these are also common weaknesses found in other wireless technologies. Examples of these Bluetooth attacks include Bluejacking (i.e., Denial of Service (DoS)), BT-SPP-Printer-MITM (i.e., man in the middle), Bluetooth Stack Smasher (i.e., fuzzing), and BlueSnarf++/Car whisper (i.e., unauthorized direct data access) [15-19]. Each of these threats compromises the security and the privacy of the Bluetooth device. Countermeasures have been taken in recent developments of the Bluetooth specifications [13-14]. However, some major concerns have to be reviewed in order to successfully understand the current weaknesses. The following list shows some of the vulnerabilities found in current studies [12-15, 18 and 19]. Countermeasures for some threats will be given in relation to the specific version of the Bluetooth specification:

- If the encryption keystream is not refreshed before 23.3 hours it will be repeated. Bluetooth v2.1 + EDR and later versions provide a periodical refreshing of the encryption keys.
- Privacy is compromised when the Bluetooth device address (BD_ADDR) is obtained. Bluetooth v4.0 provides a privacy feature making it more difficult to track and identify a device.
- Interference or jamming – does not frequently occur in Bluetooth technology since in the AFH scheme all channels (79 in total) must be blocked. The low energy (LE) system in the Bluetooth v4.0 uses only 40 channels for the hopping scheme [14]. Therefore, it will be more susceptible to interference.
- Discoverable mode – all devices should operate in non-discoverable mode when not pairing. During the discoverable mode, an inquiring attacker could capture information such as device address, local clock and other details to establish an unauthorized connection.
- Better encryption – The E0 stream cipher algorithm is weak [15]. The use of Bluetooth v4.0 + LE is recommended since this version uses AES-CCM cryptography.
- Association models – The use of some association models could allow the device to be vulnerable to certain attacks. In the case of the association model "Just Works" (available in Bluetooth v2.1 + EDR and later versions), protection is not provided from the MITM attack [12-14]. Also, the models "Passkey Entry" and "Just Works" specifically in the

Bluetooth v4.0 + LE, do not provide protection from passive eavesdropping [14].

C. *Proposed POCT use case with HDP compatibility*

As smart phone technology advances, more features are available for communicating with the phone due to the need to access data and media on the Internet. Current medical devices are being developed with various interface options to monitor (store, save, export, etc.) data. In many of these scenarios the smart phone becomes the main computation and communication engine in a POCT scheme [7, 11]. In terms of hardware, the challenges in these configurations are mainly the limitations in the interfaces provided by the smart phone, technical difficulties (required cables, connectors, and power requirements) that arise when many medical devices are connected for simultaneous use. In order to address these problems we propose the simple piconet configuration shown on Figure 2.

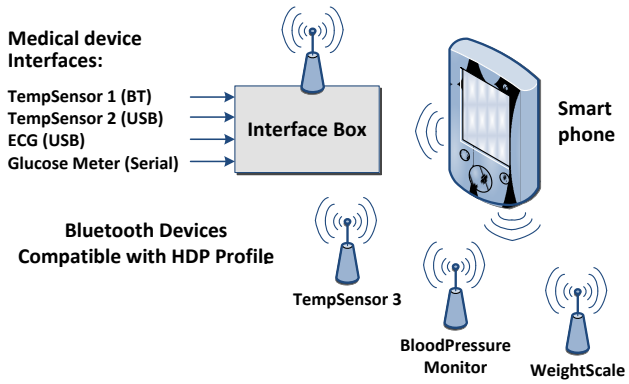

Figure 2. Proposed piconet (with the interface box).

In Figure 2, the phone serves as the master (data sink in HDP terminology) for all medical devices connected to the piconet composed of 4 slaves. The first slave in the piconet is an interface box that communicates with legacy systems (USB, Serial, Bluetooth interfaces), translates their data to IEEE 11073 data format, and then uses the Bluetooth HDP profile to send the data to the smart phone. Since these legacy systems only communicate through proprietary protocols (software) and are not interoperable, the interface basically provides the translation of the data to IEEE 11073 and provides a secure channel to privately send all the information to the smart phone. The other slaves in the piconet communicate directly to the smart phone assuming that they are already compatible with the Bluetooth HDP profile.

By using the HDP profile [11], the interface box can reset itself each time it detects a change in the medical devices attached and reconfigure itself to provide the other end (in this case the smart phone) with the proper services and data format available. The HDP profile provides a protocol stack that includes a Service Discovery Protocol (SDP), which is responsible for maintaining records of each service available. Each record contains information about the attributes of each service, the type of service offered, and any mechanism/protocol needed for its utilization.

Figure 3 shows a sample endpoint that implements multiple functions [7]. In this example, the SDP server on the interface box will maintain all the information regarding the local endpoint, which is actually implementing two example functions: glucose meter and BPM. This information will be sent to the smart phone if the SDP client issues an SDP request to the interface box. Then after receiving all the information, it configures the proper values for control and the data channels needed for the exchange. The interface box takes advantage of the flexibility available of the HDP profile to appear as a single device that provides one or multiple functionalities.

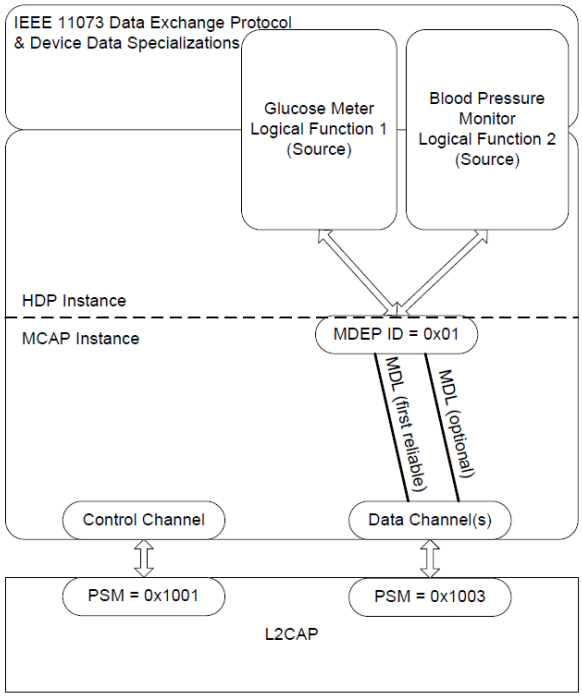

Figure 3. Multifunction device with a single logical endpoint [7].

Figure 4 shows a flow diagram that describes the main functionalities of the interface box. As the interface box is turned on it retrieves the last configuration used. This information includes all the details that are necessary to reestablish a connection between the interface box and the smart phone without requiring redundant pairing procedures.

The device then goes to the ready state, in which the interface box is prepared to perform any of the following functions:

- Driver Update – Procedure triggered when the configuration of the interface box changes, and the current protocols and drivers need to be updated. See Figure 5 for more details.
- Transfer Event – Transfer data from one or more of the devices attached to the smart phone. The interface box is triggered to enter into this procedure once it receives a request from one of the following: a medical device (attached to the interface box) or the smart phone. See Figure 5 for more details.

- Pair Device – Bluetooth pairing procedure for the initial time and each time the configuration of the interface box changes. See Figure 6 for more details.
- Software Update – Goes to firmware/drivers update procedure. Since the communication with legacy systems depend on proprietary protocols, the interface box needs to have a database of drivers for each supported medical device. Both the firmware (interface box main software) and the drivers' database need to be updated to include the new medical devices available. See Figure 6 for more details.

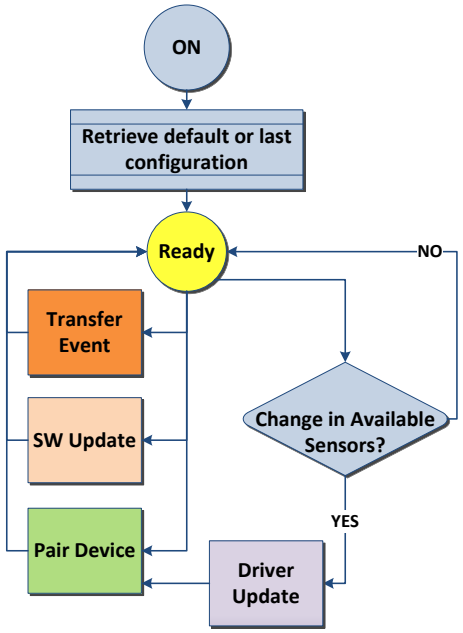

Figure 4. Interface box functional flow diagram - main operations.

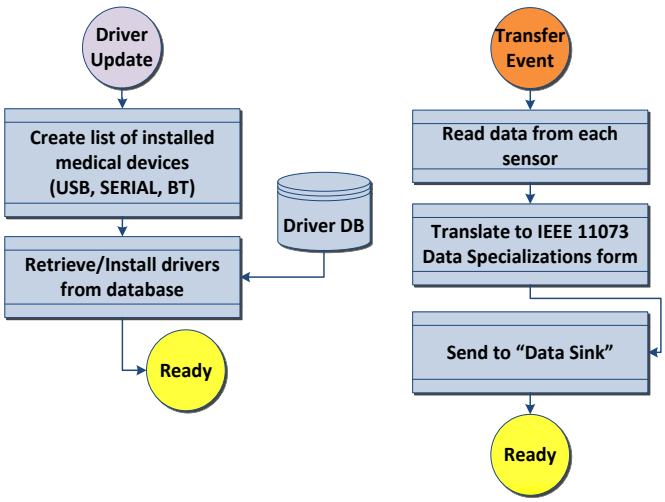

Figure 5. Interface box functional flow diagram – driver update and transfer event procedure.

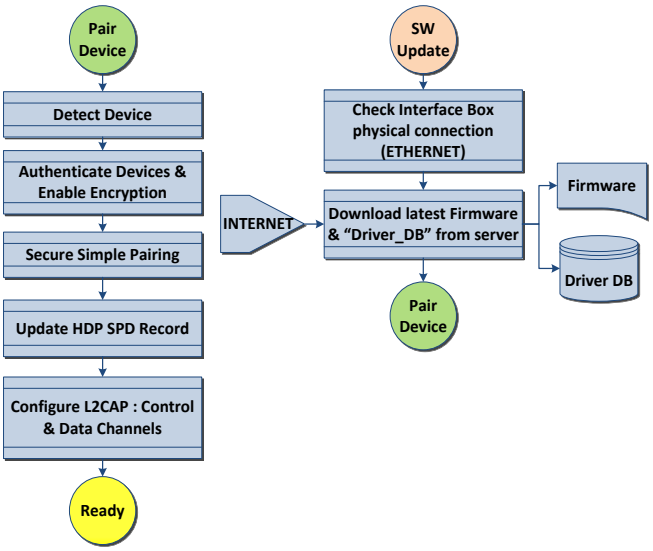

Figure 6. Interface box functional flow diagram – pair device and SW update procedures.

V. CONCLUSION

The taxonomy revealed that the RS232, USB, and Bluetooth are the output interfaces most used among medical devices. Only 10 out of the 245 medical devices in the study are currently compatible with the IEEE 11073 standard and certified by the Continua Health Alliance. The glucose meter, blood pressure monitor, system multifunctional, ECG, and pulse oximeter are the categories of medical device most commonly produced today according to the taxonomy. This study showed that among the top medical devices produced, Bluetooth is the wireless technology that is being adapted into the majority of current/new medical device designs.

A POCT system involving the use of a smart phone as the platform takes advantage of the portability, the computational power, and the communication bandwidth available on those devices. It is also important to mention that current smart phones include Bluetooth technology. Future implementations could make use of the newer Bluetooth v4.0 + LE standards to take advantage of power consumption and the IEEE 11073 interoperability included in the HDP profile. The incorporation of these standards in the next generation of POCT is vital for compatibility and interoperability.

The ability to improve security and privacy issues are the primary goals for future POCT applications. The addition of the Bluetooth HDP makes the home-based health care environments feasible and provides them with both privacy and interoperability between multiple medical devices. But only 8 out of the 245 studied medical devices (about 3%) are currently compatible with the HDP. This reveals that most of the medical devices available that use Bluetooth communication either do not support HDP or implement earlier versions of the Bluetooth specifications (earlier than v2.1 + EDR) compromising the security and interoperability between the devices. The proposed interface box will

facilitate a transition mechanism between legacy medical devices and new designs compatible with the IEEE 11073 standard. This step is important to promote the acceptance of new devices along with the use of all the current devices (not compatible with IEEE 11073), which actually compose the majority of the medical devices available today.

REFERENCES

[1] C. P. Price, A. St. John, and J. M. Hicks, *Point-of-Care Testing*, C. P. Price, A. St. John, and J. M. Hicks, Eds., 2nd ed. AACC, 2004, pp. 3-9, 459-465.

[2] *Health Informatics – Personal Health Device Communication Part 20601: Application Profile – Optimized Exchange Protocol*, IEEE Standard 11073-20601, 2008.

[3] *Health Informatics – Personal Health Device Communication Part 104xx: Device Specialization*, IEEE Standard 11073-104xx, 2008.

[4] *ISO/IEEE Health Informatics – Point-Of-Care Medical Device Communication Part 10101: Nomenclature*, IEEE Standard 11073-10101, 2004.

[5] Continua Health Alliance - http://www.continuaalliance.org/

[6] "Device Class Definition for Personal Healthcare Devices", ver. 1, USB Implementers Forum, Nov 2007. http://e-tools.info/project/documents/18001_19000/18520/healthcare_1.0.pdf

[7] *Bluetooth Health Device Profile Implementation Guidance Whitepaper*, Medical Devices WG, ver. 10, Dec 2009. http://www.bluetooth.com/Research%20and%20White%20Papers/HDP_Implementation_WP_V10.pdf

[8] *ZigBee Wireless Sensor Applications for Health, Wellness and Fitness*, ZigBee Alliances, March, 2009. http://www.zigbee.org/imwp/download.asp?ContentID=15585

[9] U.S. Department of Health and Human Services. "Understanding Health Information Privacy." Accessed Sep 20, 2010. http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[10] Bluetooth SIG. "Basics." Accessed Oct 1, 2010. http://www.bluetooth.com/English/Technology/Pages/Basics.aspx

[11] *Bluetooth Health Device Profile Specification*, ver. 10, Bluetooth SIG, Jun 2008. http://www.bluetooth.com/Specification%20Documents/HDP_SPEC_V10.pdf

[12] *Bluetooth Specification v2.1 + EDR*, vol. 0, Bluetooth SIG, Jun 2008. http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx

[13] *Bluetooth Specification v3.0 + HS*, vol. 0, Bluetooth SIG, Apr 2009. http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx

[14] *Bluetooth Specification v4.0 + LE*, vol. 0, Bluetooth SIG, Jun 2010. http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx

[15] K. Scarfone and J. Padgette. "Guide to Bluetooth Security," NIST, Gaithersburg, MDm Special Publication 800-121, Sept 2008.

[16] Bluetooth SIG. "Security Q & A." Accessed Oct 6, 2010. http://www.bluetooth.com/English/Technology/Works/Security/Pages/SecurityQA.aspx

[17] J. P. Dunning, "Taming the Blue Beast: A Survey of Bluetooth Based Threats," *IEEE Security & Privacy*, vol.8, no.2, pp.20-27, March-April 2010.

[18] R. Bouhenguel, I. Mahgoub, and M. Ilyas, "Bluetooth Security in Wearable Computing Applications," *International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET 2008)*, pp.182-186, Nov. 2008.

[19] K. Haataja, and P. Toivanen, "Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures," *IEEE Transactions on Wireless Communications*, vol.9, no.1, pp.384-392, Jan 2010.

[20] Bluetooth SIG. "Security." Accessed Oct 6, 2010. http://www.bluetooth.com/English/Technology/Works/Pages/Security.aspx

[21] Medical and Biological Sensors and Sensor Systems: Markets, Applications, and Competitors Worldwide Accessed Sep 14, 2010. http://www.marketresearch.com/map/prod/751025.html