Dependability Analysis of a Vital Sign Monitoring Application

Marcello Cinque, Antonio Coronato, Alessandro Testa

***Abstract*—The design and realization of health monitoring applications has attracted the interest of large communities both from industry and academia. Currently many cardiac diseases are unpredictable; remote and continuous health monitoring for reliable detection of these problems becomes very useful for older people and patients. Clearly, the correct functioning of a health monitoring application is very critical for the safety of patients, hence their practical application calls for stringent dependability requirements which need to be assessed against potential failure modes.**

The paper describes a dependability analysis of a long-term wearable vital signs monitoring system which can real-time measure physiological signs such as SpO2 (saturation of arterial oxygen) equipped with Bluetooth connection. We propose a system architecture for pervasive healthcare that will open up new opportunities for continuous and reliable monitoring of assisted and independent-living residents by means of a set of services already included in Uranus middleware and of new added services to achieve a higher dependability level. Finally we propose a *Failure Mode and Effect Analysis (FMEA)* to study the possible failure modes for this kind of system and to perform the dependability analysis.

***Index Terms*—Vital Signs Monitoring, Software Reliability, Pervasive Healthcare, FMEA, Ambient Intelligence.**

I. Introduction

Wearable sensor technologies have made many improvements during the last years and have captured the interest of stakeholders from different domains like healthcare.

The medical field is one of the areas, where pervasive healthcare computing appears as a tool of growing importance and the commercial applications developed for medical and healthcare systems are rising both in number and in users [1]. A new concept in healthcare, aimed to providing continuous remote monitoring of user vital signs, is emerging.

Although a rising elderly population worldwide has led to the establishment of an increasing number of long-term care institutions, the rate of healthcare nursing personnel is growing far slower than that of growth in the elderly population. Currently many cardiac diseases are unpredictable; thus, remote and continuous monitoring for reliable detection of these problems, such as ventricular arrhythmia, becomes essentially useful especially for elderly patients with end-stage heart disease. In-home pervasive networks may assist residents and their caregivers by providing continuous medical monitoring, memory enhancement, control of home appliances, medical data access, and emergency communication.

The advances in sensor technology, as well as in communication technology and treatment of data, are the basis on which the new healthcare systems can be realized. Also, systems that are designed to be minimally invasive for health monitoring and are based on smart technologies conformable to the human body will help to improve considerably the autonomy and the quality of life of patients.

Such kinds of environment are very critical for human safety and so the related applications must be considered safety critical and such a criticality should be analyzed during the design phase. Some criticality for a long-term monitoring system of vital signs is the *battery low power*, the *WiFi disconnection*, the *sensed data not delivered*, the *sensed data corrupted*, *etc*.

This paper presents a dependability analysis of an application oriented around remote, continuous medical monitoring using medical devices. Its advantages for indoor and outdoor monitoring are described in the next sections. The proposed system allows health personnel to monitor patient's vital signs from a remote location without requiring the physician to be physically present to take the measurements.

We concern on dependability [2] as the ability to avoid service failures that are more frequent and severe than acceptable. In pervasive computing, fault tolerance techniques help us to enhance dependability and some recent projects have employed related techniques, as described in [3]. Faults in a system are unavoidable and so the systems are never totally reliable, safe, available or secure [2]. Pervasive healthcare systems need to take into account how to recover from such faults.

So, it is described a novel long-term wearable vital signs monitoring system which can real-time measure physiological signs such as SpO2 (saturation of arterial oxygen) and is fault tolerant. To perform the dependability analysis and to know the possible threats that may affect the correct functioning of health monitoring systems, this paper reports the results of a FMEA conducted to identify the failure modes of the main components composing such systems. The analysis takes advantage of our past experience and detailed field studies on the dependability of mobile devices, wireless communication technologies, such as Bluetooth, and wireless sensor networks (WSNs), and builds on such results to propose a comprehensive characterization of the problems that may affect modern health monitoring systems. The resulting FMEA table is meant to be a guidance tool to direct future research

A. Coronato and A. Testa are with National Research Council of Italy - Institute for High-Performance Computing and Networking, via P.Castellino 111, 80131, Naples - Italy, e-mail: coronato.a, alessandro.testa@na.icar.cnr.it.

M. Cinque and A. Testa are with Dipartimento di Informatica e Sistemistica, Universita di Napoli Federico II, via Claudio 21, 80125 Napoli, Italy, e-mail: a.testa@unina.it

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

efforts towards the realization of more dependable health monitoring systems.

The system presented uses an underlying middleware infrastructure, namely *Uranus* [4], which provides a set of basic services for the development of vital signs monitoring applications and also uses new services and facilities to make the system more reliable.

The rest of the paper is structured in the following paragraphs. The related work is presented in Section II; Section III describes the architecture of the long-term vital signs monitoring system. Section IV we discuss about the results on the dependability analysis of the proposed system by means of FMEA table obtained. Finally, Section V reports our concluding remarks.

II. Related Work

The number of recent research projects and commercially available systems proves the great useful of biomedical devices in the pervasive healthcare field.

In the research presented in [5], there are two main architectures for ambulatory vital signs monitoring systems, which use the mobile device with a direct link (wireless, usually Bluetooth) to the wearable sensors.

A large number of monitoring systems, whose effectiveness and convenient economic impact have been widely demonstrated (e.g. [6]), have been realized for many diseases. Concerning, for example, cardiovascular diseases, which represent the leading cause of death worldwide, many wearable and portable eHealth systems have been developed (e.g. [7] [8]) [9]. The non-invasive monitoring capability of these systems concerns not only the prevention of cardiovascular diseases (e.g. myocardial infarction and stroke), but also their management, as in the case of chronically ill patients.

In [10] a ZigBee sensor data collection network is the basis of the acquiring system, being responsible for routing all data to a server. The received data are then available to be visualized either through a web browser or through a PDA based application. Chen et al. [11] described monitoring of a set of vital signs based on mobile telephony and internet.

Although there are many papers that have proposed systems for monitoring vital signs, currently there is still no system to ensure reliable and continuous monitoring even when a patient is in motion (inside and outside the home). Moreover, in literature, to properly evaluate a process or product for strengths, weaknesses, potential problem areas or failure modes, and to prevent problems before they occur, a **Failure Modes and Effects Analysis (FMEA)** can be conducted. FMEA is a team-based, systematic and proactive approach for identifying the ways that a process or design can fail, why it might fail, and how it can be made safer [12]. The purpose of performing an FMEA, as described in US MIL STD 1629 [13], is to identify where and when possible system failures could occur and to prevent those problems before they happen. If a particular failure could not be prevented, then the goal would be to prevent the issue from affecting health care organizations in the accreditation process.

An FMEA provides a systematic method of resolving the questions: *"How can a process or product fail? What will be the effect on the rest of the system if such failure occurs? What action is necessary to prevent the failure?"*. It represents a procedure for analysis of potential failure modes within a system for classification by the severity and likelihood of the failures. To realize a FMEA, the system is divided in components/functions that are divided in subcomponents/subfunctions; it considers a table in which the rows are composed by the subcomponents/subfunctions and the columns represent respectively the failure modes, the possible causes and the possible effects.

The FMEA team determines, by failure mode analysis, the effect of each failure and identifies single failure points that are critical. It may also rank each failure according to the criticality of a failure effect and its probability of occurring. There are a number of reasons why this analysis technique is very advantageous. Here are just a few:

- FMEA provides a basis for identifying root failure causes and developing effective corrective actions;
- The FMEA identifies reliability and safety critical components;
- It facilitates investigation of design alternatives at all phases of design;
- It is used to provide other maintainability, safety, testability, and logistics analyses

Since FMEA is effectively dependent on the members of the team which examines the failures, it is limited by their experience of previous failures. If a failure mode cannot be identified, then external help is needed from consultants who are aware of the many different types of product failure. FMEA is thus part of a larger system of quality control, where documentation is vital to implementation. In our case, we based the analysis both on our previous studies on different system components (such as WSNs, smart phones, and short range communication technologies) and on FMEA results available on some subcomponents, such as medical devices.

III. System Architecture

This section presents the system architecture (see figure 1) developed on top of *Uranus* [4] which performs a long-term monitoring of vital signs.

This system has been realized to monitor long-term (e.g. for 48 hours) the value of the oxygen in the blood of a chronically ill patient. A residential gateway is deployed at the home of the patient, although the monitoring must continue even when the patient is at work or elsewhere outside the home. This rises the need of handling implicit requirements like the power consumption of battery driven devices, network switching, and reliability assurance.

The system includes an oximeter, equipped with Bluetooth connection, permanently attached to the patient, which senses the value of the oxygen and transmits it to a PDA. The PDA, in turn, forwards data to the residential gateway. Data are transmitted either over the WiFi domestic network while the patient is at home, or over the GPRS network otherwise. The system must be able to detect connection failures when the patient leaves the house; i.e. it must switch from the WiFi connection to the GPRS connection. On the contrary, when the patient comes back home, the system must reuse the WiFi domestic connection.

Current implementation integrates the resources described

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

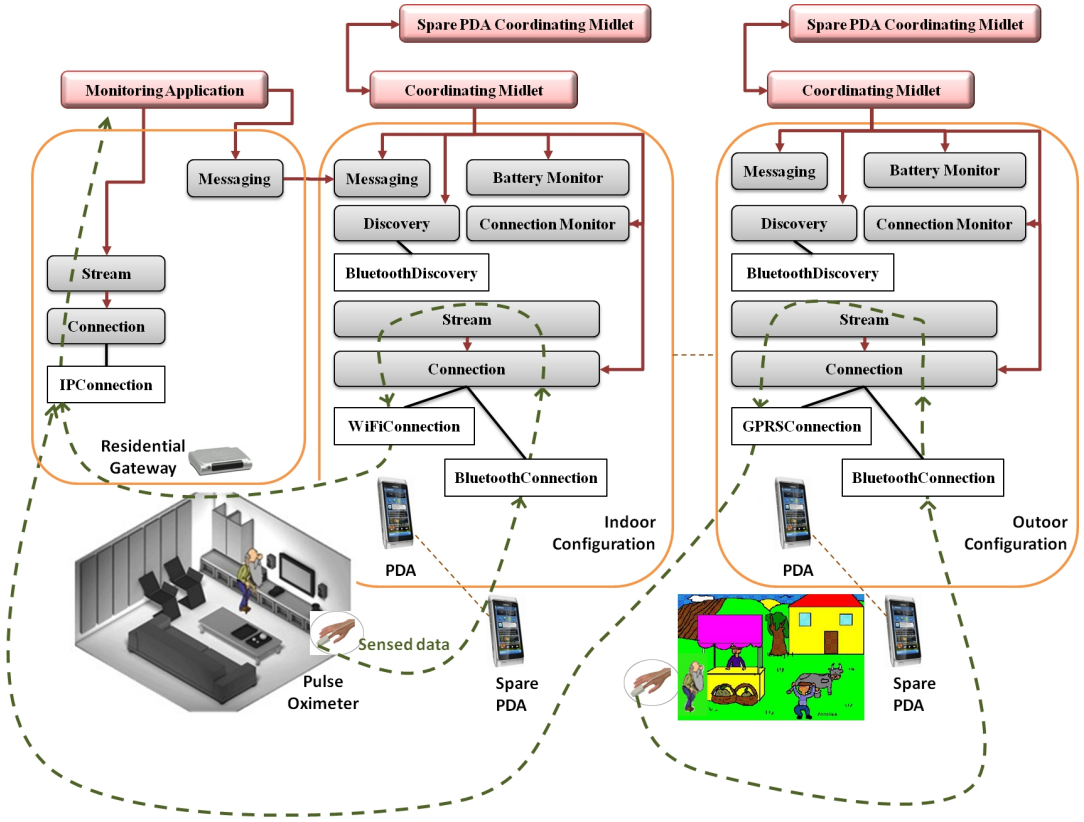

Fig. 1. System architecture

TABLE I
HW RESOURCES

	Producer	**Model**
PDA	Nokia	N8
Oximeter	Alive Tech. Pty.	Alive Pulse Oxim.

in table I. Another important issue concerns the power consumption of battery driven devices, which is a limiting factor for long-term monitoring. Although the emerging of new technologies [14] and new standards like the bluetooth low energy profile, this issue can not be considered definitively solved [15]. For this reason, the system must be able to detect low battery levels and to migrate onto spare devices.

To realize this system we have implemented new services and facilities in addition to those offered by Uranus; they are useful to add new functionalities: the management of the different kinds of communication (Bluetooth, WiFi and GPRS), the inquiry (by means of the Bluetooth communication) of medical devices to use for the monitoring, the level of the PDA's battery and finally the switch of the connection type (WiFi -> GPRS and vice versa). By means of these added modules, we are able to tackle dependability issues for these systems.

The new Services and Facilities are *BatteryMonitor* (Service) checks the level of the battery of the PDA, *ConnectionMonitor* (Service), *Discovery* (Service) provides the BluetoothDiscovery, *BluetoothDiscovery* (Facility) looks for the devices with Bluetooth enabled, *IPConnection* (Facility) to realize a communication between the residential gateway and the PDA through a WiFi or GPRS connection, *WiFiConnection* (Facility) to realize a WiFi connection when patient is at home, *BluetoothConnection* (Facility) to realize a communication between the PDA and the medical device (SpO2) equipped with Bluetooth connection and *GPRSConnection* (Facility) to realize a GPRS connection when patient is not at home. We can assume that the patient is equipped with one (or even more) spare PDA. When the level of the battery of the primary PDA reaches a certain threshold, the *Battery Monitor Service* alerts the *Coordinating Midlet*, which sends a message -through the Messaging Service- requiring the turning on of the spare PDA. Next, the two coordinating midlets start a coordination protocol. In particular, they discover each other by means of the *Discovery Service*. Then, the primary PDA releases its bluetooth and WiFi connections, while the spare PDA starts to handle the data stream.

The PDA receives data -sensed by the oximeter- through a *Bluetooth Connection* facility. Next, the PDA's *Stream Service* transmits the data to the Residential Gateway's *Stream Service* either through a *WiFi Connection*, while the patient is at home, or a *GPRS Connection* if the patient is elsewhere. Finally, the data stream is received and analyzed by a *Monitoring Application* built on top of the residential gateway. The *Connection Monitor* surveys the availability of the domestic WiFi. In particular, in the case of the patient leaving home, the *Connection Monitor* detects the WiFi disconnection fault and requires the *Connection*

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Service to start a GPRS connection. In contrast, when the patient comes back home, the *Connection Monitor* reveals the availability of the domestic network and imparts the *Connection Service* to which from the *GPRS Connection* to a *WiFi Connection*.

IV. Dependability Analysis

In this section we present the results of the FMEA we performed on vital sign monitoring application introduced in the previous section. The most frequent failure occurrences have been derived from past experiences on real architectures and from the existing literature, trying to relate failure occurrences with potential causes (faults).

The results are summarized in Table II. We prefer to focus on the components which have to be used by patients, who might not be technology experts and who need to rely on a monitoring system able to work despite the occurrence of accidental failures.

In particular, we focus on technology-related failures, such as, failures due to hardware faults, software faults, or communication problems. Failures due to physical damage of nodes (e.g. physical crashes due to accidents or very adverse weather conditions), malicious activities (e.g. manual, and unexpected, node withdrawal or substitution), and security threats are excluded from the analysis.

For each component/function (sub-component/sub-function if it is present) of the system, failure modes, potential effects and possible causes are reported.

We identified three components/functions: the node (i.e., the sensor used to monitor the patient), the Intra BAN (Body Area Network) communication and the gateway (i.e., the smartphone of the patient). Five sub-components/sub-functions have been identified for the *node* component: the sensor board, the power supply unit, the CPU, and the OS (such as [16][17] which are used in medical devices) are the general components of a node, and their analysis is based on our previous study on sensor networks [18]. In addition, we considered the failures of some specific medical device, such as the oximeter. The failures of such device have been identified starting from existing studies. Clearly, other devices can be added to the analysis if used in a specific setting.

Two sub-components/sub-functions have been identified for the *Intra BAN* function: Bluetooth stack and Bluetooth channel. These are based on our previous studies on sensor networks and on the Bluetooth protocol [18] [19]. Finally, two sub-components/sub-functions have been identified for the *Gateway* component: the device (i.e., the smartphone, starting from our previous experiences on smartphone failures [20]), and the Bluetooth application, which is responsible to gather the measurements from Bluetooth medical devices (in facts, the majority of wireless medical devices use Bluetooth as the communication technology). In [19] we noticed that several failures may affect Bluetooth applications, due to problems of the underlying Bluetooth modules.

In the following, we detail the analysis performed for each identified component/function.

A. Node (generic medical device components)

From the prospective the mission of the BAN, a node is failed when i) it is no longer able to deliver its measurements to the gateway, and ii) it is not longer able to provide meaningful measurements. This can be due the malfunction of one of the components of the node, as detailed in the following.

1) Sensor Board: we assume the sensor board can fail according to three failure modes: *stuck-at-zero*, *null reading* and *out-of-scale reading*. A stuck-at-zero of the sensor board produces the effect of a out-of-order device, which does not deliver any outputs to external inputs. Potential causes lay into faults of the sensing hardware (e.g., as can be observed in [21], the humidity sensor produces a short circuit, causing a high current drain which turns off the overall node).

Null readings cause the sensor to deliver null output values, for a certain interval of time. This may be caused by temporary short circuits that also cause the node to drain excessive power from batteries, hence shortening the overall lifetime of the node [21]. Out-of-scale readings cause the sensor board to provide no meaningful outputs, for a certain interval of time.

2) Power Supply: the power supply component may exhibit stuck-at-zero as well as reset failure modes (i.e., the node shutdowns and restarts itself). The former is due to battery energy exhaustion. The latter can be caused by anomalous power requests that cannot be supplied by batteries, e.g. the residual charge is not sufficient to provide the required amount of power.

3) CPU: the micro-controller can be affected by temporary or permanent failures, which prevent it to work correctly, hence delivering constant outputs.

4) OS: software defects (bugs) or single event upsets (bit flips) may corrupt the state of the embedded operating system, causing the whole device to hang.

B. Node (specific medical device components)

1) Oximeter: possible hazards are incorrect readings due to short circuits or too much current. This can be due to skin contacts of the oximeter, which in turn may cause irritation or rash of patient's skin. The device receives a shock and stops to function. In these cases, it is needed to reboot choose an adhesive or an electrolyte with low likelihood of reaction.

C. Intra-BAN

1) Bluetooth Stack: the Bluetooth software stack is corrupted due to faults into one of its modules, such as L2CAP, BNEP, RFCOMM, etc.

2) Bluetooth Channel: three Bluetooth channel level (i.e., the Baseband level) failures have been identified: Baseband header corruption, length mismatch, i.e., a mismatch between the packet length reported into the Baseband header and the actual one, and Baseband payload corruption. These failures are due to packet corruption and can in turn cause wrong readings or packet loss at the higher levels.

D. Gateway

1) Device (the smartphone): an analysis of the main failure modes of smart phones, performed in [20], revealed

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE II
FAILURE MODE AND EFFECT ANALYSIS OF THE VITAL SIGN MONITORING APPLICATION

Component	Sub-component	Potential Failure Mode	Potential Effects of Failure	Potential Causes of Failure
Node (the medical sensor)	**Sensor Board**	Stuck at Zero	The device is out-of-order; it does not deliver any output to inputs	Sensing hardware
		Null Reading	The device delivers null output values	Sensing hardware
		Out of Scale Reading	The device delivers no meaningful values	Sensing hardware
	Power supply	Stuck at Zero	The device is out-of-order; it does not deliver any output to inputs	Natural energy exhaustion
		Reset	The node resets itself to its initial conditions	Anomalous current request that cannot be supplied by batteries
	CPU	Stuck at Zero	The device is out-of-order; it does not deliver any output to inputs	Micro-controller
	OS	Software Hang	The device is powered on, but not able to deliver any output	Operating system's corrupted state
	Oximeter	Incorrect reading	Wrong data values, irritation or rash of skin	Skin contact
Intra BAN Communication	**Bluetooth Stack**	Bluetooth stack failure	A Bluetooth module (e.g. L2CAP, BNEP, etc.) fails	Bluetooth stack's corrupted state
	Bluetooth Channel	Header corruption	Header delivered with errors	Packet corruption
		Header length mismatch	Header length deviates from the specified one	Packet corruption
		Payload corruption	Payload delivered with errors	Packet corruption
Gateway	**Device (the smartphone)**	Freeze	The device's output becomes constant; the device does not respond to the users input.	Systems corrupted state
		Self-shutdown	The device shuts down itself; no service is delivered at the user interface.	Natural energy exhaustion or self-reboot due to corrupted state
		Unstable behavior	The device exhibits erratic behavior without any input inserted by the user	System/Application corrupted state
		Output failure	The device delivers an output sequence that deviates from the expected one	System/Application corrupted state
		Input failure	User inputs have no effect on device behavior	System/Application corrupted state; Natural energy exhaustion
	Bluetooth Application	Inquiry/Scan Failure	The scan procedure terminates abnormally	A Bluetooth module fails or device out of range
		Discovery Failure	The discover procedure terminates abnormally	A Bluetooth module fails or device out of range
		Connect Failure	The device is unable to estabilish a connection	A Bluetooth module fails or device out of range
		Packet Loss	Expected packets are not received	Packet corruption
		Data mismatch	Packets are delivered with errors in the payload	Memoryless channel with uncorrelated errors

that these device may exhibit several failures, due to both hardware issues and software defects. Specifically, five failures have been identified: freeze (the device is completely blocked, and only pulling-out the battery restores proper operation), self-shutdown (the device resets itself due to battery exhaustion or reaction to a system corrupted state), unstable behavior, output failure, and input failure (due to system or application corrupted states).

2) Bluetooth Application: the application governing the Bluetooth communication may exhibit a variety of failures according to the utilization phase where they occur, i.e., inquiry/scan and discovery phases, connection, and data transferring. Failures during the connection can occur either while the connection is set up or while the role of the device is switched from master to slave. Unexpectedly, failures during data transfer, such as packet loss and mismatches in the received data, are experienced, despite error control mechanisms performed by Baseband. Correlated errors (e.g. bursts) can occur due to the nature of the wireless media, affected by multi-path fading and electromagnetic interferences.

All of these analyzed failures cause abnormal vital sign readings; health monitoring systems must be aware of all the possible failures, in order to react to them or, at least, to detect them. For instance, in case of failure detection, a possible action can be to call to the patient's home or to call to an emergency contact to suddenly check the patient status and restore the normal operation of the system.

Also we are able to deduce some results on the dependability of the presented vital sign monitoring application. We focus on the fault coverage.

We consider four types of faults:

- *Battery low power*
- *WiFi disconnection*
- *Sensed data not delivered (on the time)*
- *Sensed data corrupted*

Concerning the first two types of faults, the system, being equipped with battery and connection monitors along with additional logic for coordinating the spare PDA, is able both to detect and recover the fault. In addition, if the system

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

is equipped with a timer (also available in Uranus) for monitoring the delay and jitter of transmitted data, it will also be able to detect excessive delay in the transmission of vital signs. However, with the current architecture there is no mechanism for recovering from this fault. Finally, in the case of sensed data corrupted, the system is not able to detect the fault and then recover it.

V. Conclusion

Vital signs monitoring is a field of application that is receiving great attention from several kinds of stakeholder interested in the realization of systems and applications which are effective, reliable, economically convenient, and capable of improving the quality of life for patients.

It has been considered a a long-term vital signs monitoring system that can measure various physiological signs, such as SpO2. The system allows health personnel to monitor a patient from a remote location without requiring the physician to be physically present to take the measurements and also is able to detect and recover some fault that may occur such as battery low power, WiFi disconnection, sensed data not delivered and sensed data corrupted.

We conducted a Failure Mode and Effect Analysis to perform a dependability analisys of a vital sign monitoring application. The analysis considered the main components and the main medical devices that are considered for the application, and it is based partially on our previous experience and studies on some of the components, i.e., Bluetooth, sensor networks, and smart-phones, and partially on the results already available for medical devices.

Even if the analysis represents only a base for further studies, it reveals that several failure modes are usually neglected by current health monitoring solutions, where only node crashes are considered, hence exposing patients to potential health risks; we believe this system design will greatly enhance quality of life, health, and security for those in assisted-living communities.

Future efforts will be devoted to the definition of architectural solutions for this kind of health monitoring systems, able to take into account the failure modes identified in the this paper, and capable to detect failures at runtime in order to propose proper countermeasures, toward the goal of building more dependable health monitoring systems in the future.

References

[1] J. Sarashon-Kahn, "How smartphones are changing health care consumers and providers," *California Health Foundation*, 2010.

[2] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secur. Comput.*, vol. 1, pp. 11–33, January 2004. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2004.2

[3] S. Chetan, A. Ranganathan, and R. Campbell, "Towards fault tolerance pervasive computing," *Technology and Society Magazine, IEEE*, vol. 24, no. 1, pp. 38 – 44, spring 2005.

[4] A. Coronato and A. Testa, "Runtime verification of location-dependent correctness and security properties in ambient intelligence applications," pp. 153 –160, feb. 2011.

[5] J. Rodriguez, A. Goni, and A. Illarramendi, "Real-time classification of ecgs on a pda," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 9, no. 1, pp. 23 –34, march 2005.

[6] A. Darkins, P. Ryan, R. Kobb, L. Foster, E. Edmonson, B. Wakefield, and A. E. Lancaster, "Care Coordination/Home Telehealth: The Systematic Implementation of Health Informatics, Home Telehealth, and Disease Management to Support the Care of Veteran Patients with Chronic Conditions," *Telemedicine and e-Health*, vol. 14, no. 10, pp. 1118–1126, Dec. 2008. [Online]. Available: http://dx.doi.org/10.1089/tmj.2008.0021

[7] J. Cleland, A. Louis, A. Rigby, U. Janssens, and A. Balk, "Noninvasive home telemonitoring for patients with heart failure at high risk of recurrent admission and death: the trans-european network-home-care management system (ten-hms) study," *Journal of American College of Cardiology*, vol. 45, may 2005.

[8] R.-G. Lee, K.-C. Chen, C.-C. Hsiao, and C.-L. Tseng, "A mobile care system with alert mechanism," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 11, no. 5, pp. 507 –517, 2007.

[9] A. Mortara, G. Pinna, P. Johnson, R. Maestri, S. Capomolla, M. La Rovere, P. Ponikowski, L. Tavazzi, and P. Sleight, "Home telemonitoring in heart failure patients: the hhh study (home or hospital in heart failure)," *European Journal of Heart Failure*, vol. 11, no. 3, 2009.

[10] P. Khanja and S. Wattanasirichaigoo, "A web based system for ecg data transferred using zigbee/ieee technology," *Journal of Medical Systems*, vol. 31, pp. 467–474, December 2007.

[11] W. Chen, S. Tokinoya, and N. Takeda, "A mobile phone-based wearable vital signs monitoring system," in *Proceedings of the The Fifth International Conference on Computer and Information Technology*, ser. CIT '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 950–955. [Online]. Available: http://dx.doi.org/10.1109/CIT.2005.19

[12] R. J. Latino and A. Flood, "Optimizing fmea and rca efforts in health care," *Journal of Healthcare Risk Management*, vol. 24, no. 3, pp. 21–28, 2004. [Online]. Available: http://dx.doi.org/10.1002/jhrm.5600240305

[13] "Us mil std 1629 1980: Procedure for performing a failure mode, effect and criticality analysis, method 102," November 1980.

[14] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power management in energy harvesting sensor networks," *ACM Trans. Embed. Comput. Syst.*, vol. 6, September 2007. [Online]. Available: http://doi.acm.org/10.1145/1274858.1274870

[15] Y. Zhang and H. Xiao, "Bluetooth-based sensor networks for remotely monitoring the physiological signals of a patient," *Trans. Info. Tech. Biomed.*, vol. 13, pp. 1040–1048, November 2009. [Online]. Available: http://dx.doi.org/10.1109/TITB.2009.2028883

[16] "Qnx." [Online]. Available: http://www.qnx.com/solutions/industries/medical/

[17] "Threadx." [Online]. Available: http://www.qnx.com/solutions/industries/medical/

[18] M. Cinque, D. Cotroneo, C. D. Martinio, and S. Russo, "Modeling and assessing the dependability ofwireless sensor networks," *Reliable Distributed Systems, IEEE Symposium on*, vol. 0, pp. 33–44, 2007.

[19] G. Carrozza and M. Cinque, "Modeling and analyzing the dependability of short range wireless technologies via field failure data analysis," *Journal of Software*, vol. 4, no. 7, 2009. [Online]. Available: http://ojs.academypublisher.com/index.php/jsw/article/view/0407707716

[20] M. Cinque, D. Cotroneo, Z. Kalbarczyk, and R. Iyer, "How do mobile phones fail? a failure data analysis of symbian os smart phones," in *Dependable Systems and Networks, 2007. DSN '07. 37th Annual IEEE/IFIP International Conference on*, june 2007, pp. 585 –594.

[21] R. Szewczyk, J. Polastre, A. Mainwaring, and D. Culler, "Lessons from a sensor network expedition," 2004, pp. 307–322.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)