Managing Criticalities of e-Health IoT Systems

Ch. Kotronis, G. Minou, G. Dimitrakopoulos, M. Nikolaidou, D. Anagnostopoulos
Department of Informatics & Telematics,
Harokopio University of Athens, Athens, GREECE.
{kotronis, gminos, gdimitra, mara, dimosthe}@hua.gr

A. Amira, F. Bensaali, H. Baali, H. Djelouat
College of Engineering,
Qatar University, Doha, QATAR
{abbes.amira, f.bensaali, hamza.djelouat, hamza.baali}@qu.edu.qa

***Abstract*—Lately, Internet-based solutions, brought by the Internet of Things (IoT) and cloud computation and storage technologies, have been driving revolutionary approaches in innumerable domains, including the sensitive domain of healthcare. Indicatively, real-time diagnosis of medical issues, telemedicine, remote monitoring of patients, as well as computer-assisted smart transportation in case of emergencies, are anticipated as Systems-of-Systems (SoS) that can execute several applications of different criticality, thus necessitating mission-critical and non-critical peripheral components. Therefore, managing the criticality of a specific component, application or service in such an environment, is of fundamental importance. In this respect, this paper discusses an approach to identify and model criticalities of healthcare IoT systems, as a first step to effectively manage them in system implementation and deployment. To do so, it explains the mixed-criticality characteristics of such systems, describing two principal use cases, that stem from the combination of novel technologies with classic health care practices, namely (a) a remote elderly monitoring platform, as well as (b) a smart ambulance system. The main cricalities anticipated in such systems are described, as well as open areas for future research are also identified.**

***Index Terms*—Internet of Things, e-Health Services, Criticalities, Remote Elderly Monitoring, Smart Ambulance Systems**

I. Introduction

In our modern era, the Internet governs almost every aspect of our daily lives. In recent years in particular, Internet-based solutions have been applied in the sensitive domain of health care and medicine. The advent of the Internet of Things (IoT), the rise of the Cloud and on-demand computation and storage, as well as the proliferation of sensors and ubiquitous wireless communication are expected to drive revolutionary approaches in health care activities such as: real-time diagnosis of medical issues, telecare and telemedicine, remote monitoring of patients, as well as computer-assisted smart transportation in case of emergencies. Such approaches can be implemented via new types of Systems-of-Systems (SoS), which are mainly composed of hardware (e.g., sensors, smartphones) and software (e.g., specialized OSes, Cloud services) that can execute several applications of different criticality [1].

Health care is traditionally a domain requiring mostly safety-critical core systems and functionalities, since human lives can be jeopardized by a faulty implementation. Moreover, the complex information and communication technology (ICT) involved may also include mission-critical [2] or non-critical peripheral components. Identifying the criticality of a specific IoT component, application or service in complex smart health-care systems is of significant importance for the effective implementation and support of such systems.

This paper discusses an approach to identify and model criticalities of e-Health IoT systems, as a first step to effectively manage them in system implementation and deployment. Two principal use cases, that stem from the combination of novel ICT technologies with classic health care practices, are explored identifying and explaining the mixed-criticality characteristics of the associated systems. We focus on remote monitoring and diagnosis for the sensitive demographic of elderly subjects consisting Remote Elderly Monitoring System (REMS) platform. In general, the REMS deals with the real-time diagnosis of a medical incident. Secondly, we describe a progressive Smart Ambulance System (SAS) that enables fast dispatching of ambulances to locations of medical incidents and treatment of a patient on-board with the assistance of remote health care personnel (who can make preliminary diagnosis and preparations). In general, SAS deals with the in-time delivery and treatment of a patient after a medical emergency has been identified (e.g., via the REMS).

In section II related work is briefly discussed. REMS and SAS systems are presented in sections III and IV respectively. Criticalities in both systems are identified in section V, while conclusions reside in section VI.

II. Related Work

A review of the relevant literature reveals the ongoing and increased interest in the IoT and IoT-based technologies and solutions. In [3], an overview of the IoT is presented. Regardless of the challenges, such as security, privacy, etc, that impede the progress of IoT applications, the overview highlights the significance and benefits of the Internet of Things across a range of application domains and areas. In a similar context, important aspects of the IoT are surveyed in [4], where emphasis is given on the IoT technologies and their application in the areas of transportation, logistics or health care.

Health care is becoming one of the most attractive applications

field, where the Internet of Things can offer improved access to care, increased quality and efficiency and reduced costs. As the technology for collecting, analyzing and transmitting data in the IoT continues to grow, more IoT-driven health care applications, services and systems emerge [5]. In [6], the need of an integration of IoT technologies (e.g., RFID [7] or wearable devices) and eHealth solutions is addressed. Focus is given on an integrated system for the continuous monitoring of students at risk to high blood pressure as well as a quick treatment and consultation from medical experts from a distance. Riazul Islam et al. (2015) [8], analyze a variety of more medical IoT applications, such as remote health monitoring, fitness programs or elderly care. The aforementioned were combined with architectures and platforms, like IoThNet. Relevant to the notion of remote monitoring and care, few approaches propose the use of a mixture of embedded sensors as diagnostic tools, cloud-based architectures and data analytics that would improve the quality of life of a patient and help him remain independent [9], [10]. In addition, Sebestyen et al. (2014) [11], experimented with portable devices and different communications protocols and models for the creation of eHealth applications, like the CardioNet. Moreover, in [12], a tested real-time monitoring platform that uses IoT gateways and medical devices, introduces the need of Edge Computing and shows the effectiveness of IoT in real-time eHealth services.

As the elderly have become one of the main target groups that need eHealth applications and solutions, there are frameworks that focus on making technologies more accessible to them. "Home Health Hub Internet of Things" or "H3IoT" is presented in [13] as a novel architectural framework for elderly monitoring. Furthermore, an IoT-based remote elderly monitoring study [14] introduces and analyzes an architecture where vital signs of elderly individuals are collected via sensors and monitored in real-time by a remote facility (e.g., a hospital).

There are also numerous efforts to implement Smart Ambulance systems. In [15], a system to assist a subject / patient to find the location of the nearest ambulance in case of an emergency, using a simple smartphone (Android) application. Moreover, the same system supports the transmission of the patients medical data from the ambulance (transporting the patient) to a healthcare facility. SatCare [16] is a smart ambulance system that provides real-time patient diagnosis.

III. REMS as an IoT service

In the context of this work, a remote health care monitoring system [17] is a platform that enables the doctor(s) (or in general health care provider) to monitor the health status of a patient remotely, reducing the number of times a patient has to travel for a regular check at a health care facility premises. Medical information from the patient, e.g., stemming from embedded sensors, is electronically transmitted via a secure channel to the health care provider in a different location (e.g., a hospital) for further assessment and recommendations. The doctor(s) should be alerted if theres a cause for concern, e.g., inferred symptoms of a health problem which requires immediate medical attention. The proposed system consists of a variety of diagnostic tools and devices, used for monitoring physiological signs and health parameters of the elderly in real-time, from a health care personnel located at a remote facility[18]. REMS architecture is composed of three (3) subsystems: the home (where the elderly patient resides), the data repository (where data is stored and processed) and the remote facility (where the health care personnel is located). Table I summarizes the basic services REMS offers.

TABLE I
REMS - Services

Basic Services & Applications		
Subsystem	**Service**	**Object of Service**
Home	Record	Vital signs Sleep Safety
	Transmit	Collected data
Data Repository	Storage	Collected data
Remote Facility	Detection	Abnormal signs Abnormal behavior Incidents
	Health Care	Monitoring Emergency support Communication Expert recommendation

IV. SAS as an IoT Service

The Smart Ambulance Systems targets two primary services: a) Dispatching the nearest available ambulance to an incidents location and b) provides on-line monitoring of patients and sends patient's data to the health-care facility. SAS architecture is composed of three (3) subsystems:

Ambulance Dispatch System-Monitoring Center, which finds and dispatches the nearest available ambulance to an incidents location.

Health-Care Facility. It can be a hospital, a clinic or any medical facility.

Ambulance , which responds to an emergency and provides health care to a patient en-route to the health-care facility.

Its basic functionality is the real-time monitoring of a patients medical data inside the ambulance via telecommunication services and the provision of consultation, medical advices and support. In addition, it can track the ambulance and its route. Note that in the most common scenario, the monitoring center and the ambulance are considered as components of a healthcare facility and thus belong to its infrastructure.

V. Identifying Criticalities

In this section we analyze the critical parts of REMS and SAS as mixed-criticality systems. Three (3) criticality categories are considered:

1) Safety-critical. Any failure or disruption may result in serious injury or loss of life.
2) Mission-critical [2]. It is a factor essential to a business operation or an organization. Any failure or disruption

will result in serious impact upon the organization (e.g., the organization can lose its credibility).

3) Non-critical. All the criticalities not falling in the two previous categories.

A. REMS Criticalities

Figure 1 illustrates REMS with its components (red colored) as a mixed-criticality system with safety (dark yellow colored), mission (blue-colored) and non-critical (green-colored) criticalities. Criticalities considered as both safety and mission-critical are illustrated with the light yellow color.

In the following, we discuss the identified criticalities grouped related to each discrete subsystem:

Home. All the sensors (e.g., Electrocardiogram (ECG)) are safety-critical, since failure to operate and record patient-related vital signs may result in serious harm. Lacking the appropriate redundancy on a hardware level is important. It is critical that the set of sensors should operate correctly 24/7 even in the face of individual sensor failures.

The safety critical factor applies to the gateway layer, as the real-time collection and transmission of data should be redundant with tolerance to transient failures. The gateways are responsible for the robust real-time identification and management of sensor data flows stemming from remote monitoring devices. Also, it is critical for them to possess the efficiency and technical capabilities in order to encapsulate a large number of functions (e.g., receive data from all sensors, preprocess, send data, etc) within their system.

Time is a safety-critical factor for both sensors and gateways. The results have to be generated and transmitted within a given time interval or the real-time behavior of the system is jeopardized and considered faulty.

The security is mission-critical as it may affect the credibility of the remote facility. There is a need of communications between devices that ensure the confidentiality and integrity of transmitted data without any fault or modification by an adversary.

Finally, the low power consumption of all devices can be considered as non-critical. The problem with low power consumption protocols, like Bluetooth Low Energy (BLE) 4.0, is that the security criticality might be affected in a negative way. Another non-criticality is the Size, Weight and Power (SWaP) [19] that helps ensure that devices are easier to carry and have larger autonomy.

Data Repository. The challenge in this subsystem is the management of medical data. It is critical to protect patients sensitive medical data, from the sensors to the data repository and then to the remote facility). Therefore, the following must exist, with greater weight being placed on the clouds side.

Data / Service Reliability is safety-critical. Cloud service providers need to provide excellent reliability of services over the cloud, especially in the health care industry [20]. The availability of the data is considered as safety-critical. The health care system cannot operate without availability of services and patients sensitive data.

Moreover, privacy is mission-critical. It must be guaranteed so that the health care organization can safely shift to cloud-based solutions, because of the sensitivity of the patients data. HIPAA [21] has some very strict regulations about the privacy of medical data.

Finally, flexibility is non-critical in a data repository. The cloud services should be flexible and configured according to the user requirements. Adding new services as needed should be accommodated.

Remote Facility. First, the operation and maintenance of the facilitys medical database is safety-critical with a very high significance as it holds all patients sensitive medical data and history. In practice it involves similar criticalities as in the cloud-based data repository section.

Secondly, the remote care system, as a basic part of the remote facility, is safety-critical. The operation and visualization of the patients medical data in real-time to the health care personnel is very important. The received bio-signals must be presented in textual or graphical waveforms for visualization and diagnosis purposes. In addition, it is critical for the system to support multiple different platforms for the data visualization as it is a viable market policy.

As there are not any mission and non-critical factors in the remote facility, it is characterized as safety-critical with a high significance in the REMS.

REMS as whole. In general, the REMS inherits the criticalities of its subsystems (home, data repository, remote facility). In this section, we expand on the criticalities of the REMS as an integrated system of systems.

First, the real-time monitoring process is safety-critical. The REMS has functions that must react in real-time and provide time predictable communication among different networked devices. A failure to perform an operation within a given time may result in serious harm. The significance of the real-time monitoring is very high.

Secondly, the fault isolation is also a safety-critical. Faults in an application / device must not propagate to other. Any fault must be handled by the failing application itself or by the system, while cascading failure effects should be highly improbable. The significance is between medium and high.

Safety-critical can also be the temporal isolation / correctness. The real-time behavior of an application must be correct, independently of the execution of other applications. The significance is medium / high.

The security is mission-critical. Communications between devices shall be confidential. Moreover, due to high significance of the data, the traffic leaving the devices must be encrypted, while ensuring their integrity. It is critical to avoid errors or intentional modification to the data being transmitted. For example, false measurements cannot be injected by an adversary using packet spoofing or Denial of Service (DoS) attacks. In order to meet this criticality, well-known network security protocols and software suites can be employed.

The fault information is both safety and mission-critical. The REMS platform must provide fault information to the devices, applications (lost data) and system. Information about faults occurring at the lower levels can be sent, in order to take

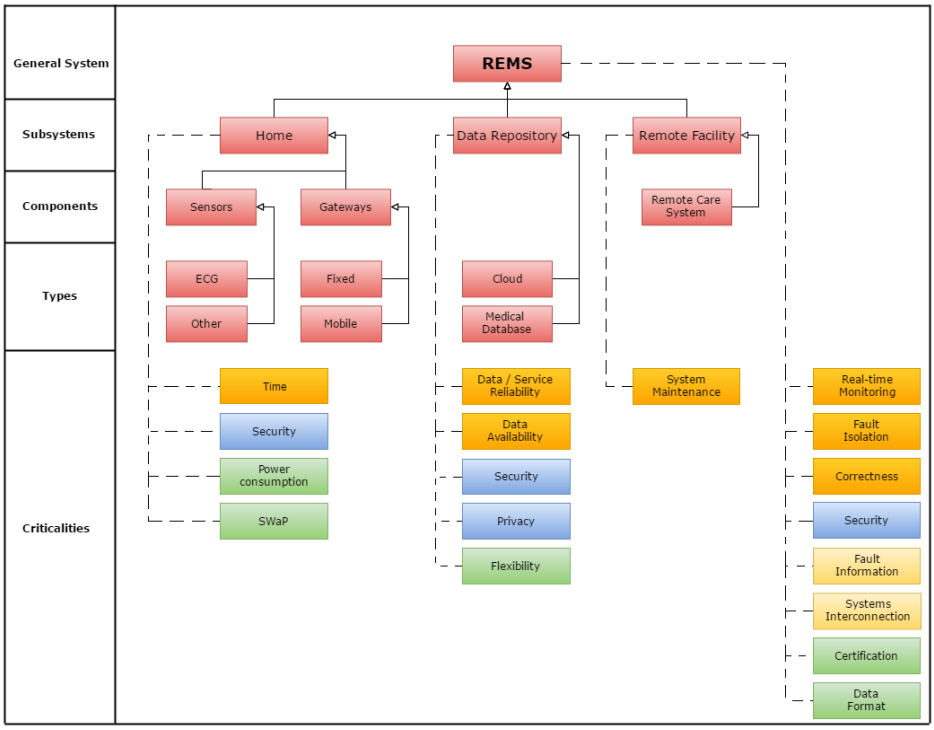

Fig. 1. REMS Subsystems,Components and Criticalities

corrective actions. Single points of failure should be avoided, and the integrated system should be distributed and highly redundant to reduce the criticality of such faults in the first place. The significance is high.

Another highly significant safety / mission-critical is the systems interconnection. All the devices (e.g., sensors, connected devices, etc) must interact and cooperate with external services.

As for the non-critical, the system should be developed while taking into account health care certifiability (e.g., HIPAA standards), for higher applicability in the health care domain. Moreover, data should have a robust and extendable standard format to be readable more or less indefinitely.

B. SAS Criticalities

Figure 2 illustrates SAS as a mixed-criticality system with subsystems in pink color and components in green color. In such a system, the following criticalities (in blue color) can be identified:

Ambulance Dispatch time. This is characterized as safety-critical, since it depends on a fast-as possible dispatch, response and arrival (to either the incidents location or a healthcare facility) of the ambulance.

Robust and reliable communication. As both a safety and a mission-critical factor, it is important for the connection between an ambulance and a healthcare facility to be always on. Moreover the communication should be secure and redundant against non-authorised adversaries.

Real-time Monitoring and Telecommunication. This is a safety-critical factor and constitutes the most important criticality for the SAS. Healthcare personnel needs to monitor and supervise the collected patients vital signs (such as heart rate, blood pressure, body temperature, etc) in real-time, using small-factor diagnostic tools, like sensors, and transmit these data to a remote healthcare facility or to a remote data repository for storage and further analysis. Further, it is necessary to monitor the patient using video and images. The vital signs of the patient are measured and placed within acceptable ranges; alarms are activated and displayed both to the ambulances screen and the healthcare personnels monitoring system in the case of patients signs are outside the specified limits.

Another safety-critical factor is the *emergency access to the patients medical record*. In case of emergency situations, the healthcare personnel might need to gain full access to a patients medical record and history in order to appropriately treat them.

Support of external consultation. It can be treated as a safety-critical factor if it involves the immediate consultation for the treatment of a patient as well as a non-critical factor in case the patient has already reached the facility and the initial emergency has been dealt with successfully.

VI. Conclusions

Recent trends in the world of communications, such as the advent of the IoT and related technologies, have paved the way for innovative healthcare services and applications. Those services and applications are often seen as Systems of Systems, which can execute several processes of different criticality, thus necessitating mission-critical and non-critical peripheral components. Therefore, managing the criticality

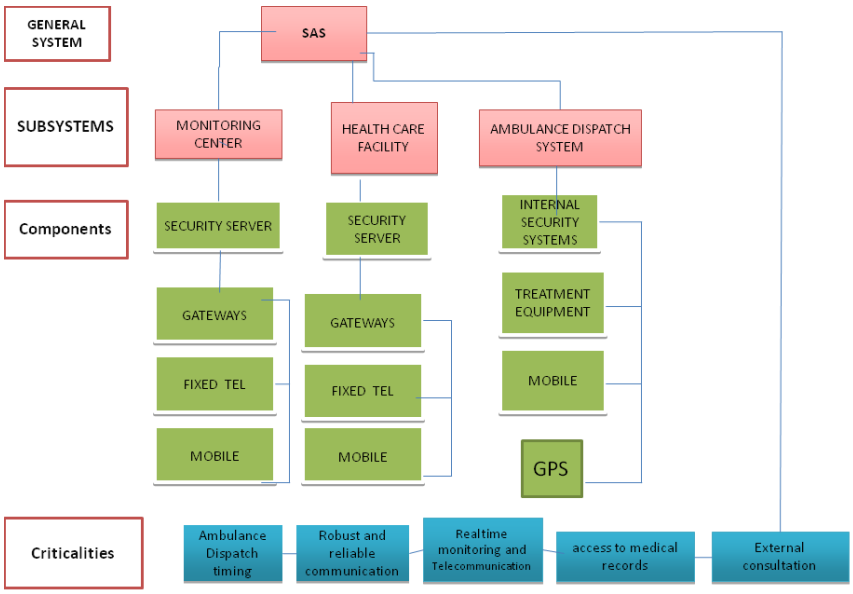

Fig. 2. SAS as a mixed-criticality system with subsystems and their components

of a specific component, application or service in such an environment, is of fundamental importance.

In this respect, this paper has discussed on an approach to identify and model criticalities of healthcare IoT systems, as a first step to effectively manage them in system implementation and deployment. To do so, the paper described some fundamental aspects on the mixed-criticality characteristics of such systems, through two principal use cases, that stem from the combination of novel technologies with classic health care practices, namely (a) a remote elderly monitoring platform, as well as (b) a smart ambulance system.

Several exciting areas are yet to be explored. First, a generic IoT architecture for supporting mixed-criticality healthcare systems shall be specified. Second, a per use case set of requirements can be further extended to include upgradable and reconfigurable parameters of each service and application. Last, additional novel healthcare oriented applications can be investigated, through the proposed mixed-criticality approach.

VII. Acknowledgement

The authors wish to acknowledge the Qatar National Research Fund project EMBIoT (Proj. No. NPRP 9-114-2-055) project, under the auspices of which the work presented in this paper has been carried out.

References

[1] A. Burns and R. I. Davis, "Mixed criticality systems-a review."
[2] F. Ciccozzi, I. Crnkovic, D. Di Ruscio, I. Malavolta, P. Pelliccione, and R. Spalazzese, "Model-driven engineering for mission-critical iot systems," IEEE Software, vol. 34, no. 1, pp. 46–53, 2017.
[3] R. Karen, S. Eldridge, and L. Chapin, "The internet of things: An overview," 2015.
[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[5] G. Carnaz and V. B. Nogueira, "An overview of iot and healthcare," 2016.
[6] T. Takpor and A. A. Atayero, "Integrating internet of things and ehealth solutions for students healthcare," vol. 1, 2015.
[7] R. Want, "An introduction to rfid technology," IEEE pervasive computing, vol. 5, no. 1, pp. 25–33, 2006.
[8] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.
[9] Z. M. Kalarthi, "A review paper on smart health care system using internet of things," International Journal of Research in Engineering and Technology, vol. 05, no. 03, p. 8084, 2016.
[10] M. P. Bharathan, M. V. Nadar, and M. S. Wayal, "Remote health monitoring using iot," 2017.
[11] G. Sebestyen, A. Hangan, S. Oniga, and Z. Gál, "ehealth solutions in the context of internet of things," pp. 1–6, 2014.
[12] H. Moustafa, E. M. Schooler, G. Shen, and S. Kamath, "Remote monitoring and medical devices control in ehealth," pp. 1–8, 2016.
[13] P. P. Ray, "Home health hub internet of things (h3iot): An architectural framework for monitoring health of elderly people," pp. 1–3, 2014.
[14] I. Azimi, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, "Internet of things for remote elderly monitoring: a study from user-centered perspective," Journal of Ambient Intelligence and Humanized Computing, vol. 8, no. 2, pp. 273–289, 2016.
[15] "Ambulance-based telemedicine saving lives in real-time."
[16] "Satcare - real-time remote diagnosis through in-ambulance ..." 2016.
[17] Medtronic, "What is remote monitoring," 2016.
[18] M. Bujnowska-Fedak and U. Grata-Borkowska, "Use of telemedicine-based care for the aging and elderly: promises and pitfalls," Smart Homecare Technology and TeleHealth, p. 91, 2015.
[19] I. THALES DEFENSE & SECURITY, "Design considerations for size, weight, and power constrained radios," 2006 Software Defined Radio Technical Conference and Product Exposition, 2006.
[20] H. A. K. Khattak, H. Abbass, A. Naeem, K. Saleem, and W. Iqbal, "Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure," 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015.
[21] HHS.gov., "Health information privacy." 2015.