Workshop Proceedings of the 11th International Conference on Intelligent Environments
D. Preuveneers (Ed.)

doi:10.3233/978-1-61499-530-2-58

A Preliminary Study of a Probabilistic Risk-based Approach for Ambient Intelligence Healthcare Systems

Giuseppe CICOTTI [a,1], Antonio CORONATO [a]
[a] *Institute for High Performance Computing and Networking ICAR-CNR Napoli - Italy*

Abstract. The Ambient Intelligence (AmI) paradigm applied to the healthcare sector is a promising solution to develop software-based systems capable of supporting medical procedures and activities carried out in a close, high-regulated, and complex healthcare environment. An AmI Healthcare System (AmI-HS) which may impact on the health and life of its users (i.e. doctors, caregivers, patients, etc.) is considered as a Medical Device (MDs), and thus subject to pass through a cumbersome risk-based regulatory process which evaluates and certifies the system safety before it is put on the market. Thus, a human-centred risk analysis is of paramount importance to establish the safety level of an AmI-HS.

In this paper, we propose a dynamic probabilistic risk assessment (DPRA) approach for AmI-HS which allows the quantitative assessment of risk in different hazard scenarios in order both to support the design and development of AmI-HSs and to provide those objective evidences needed during the regulatory process. In addition, to support our risk-based methodology we define a probabilistic risk model (PRM), based on an extension of a Markov Decision Process (MDP), capable of taking into account two main peculiarities of AmI-HSs: context-awareness and personalisation. Some preliminary results show the feasibility of our approach and the capability of our model to assess risk of context-aware hazard scenarios.

Keywords. Probabilistic Risk Assessment, Probabilistic Model Checking, Markov Decision Processes, Safety, Ambient Intelligence

1. Introduction

The pervasiveness of sensors and mobile technologies such as smartphones, personal digital assistants, tablets, etc in our daily life along with the widespread use of digital networks as the backbone by which such devices can exchange data has been allowing the advancement and promotion of software-based components everywhere all around people. Ambient Intelligence (AmI) systems exploit such technologies in order to sense the context, gather situational data, elaborate information, and support human activities in the environment in which they are carried out.

[1]Corresponding Author: Giuseppe Cicotti, ICAR-CNR, Via P.Castellino, 111 Napoli, Italy; E-mail: giuseppe.cicotti@na.icar.cnr.it

For a wider comprehension of AmI concepts and applications we refer to [1,2,3]. Instead, in this paper we narrow down our attention to AmI Healthcare Systems (AmI-HS) [4] which distinguishably present three features. First of all, the human factor plays a fundamental role because of both the wide interaction between humans and digital devices and the unique capabilities of humans in doing activities not performable by any autonomous computational system, or for which humans are considered more reliable (e.g. medical diagnosis). Secondly, AmI-HSs are distributed systems which connect and use environmental sensors and medical devices (e.g. body sensors) with the ultimate purpose of simultaneously managing and controlling both medical activities and patients' physiology in a predefined environment such as hospitals, healthcare departments, nursing homes, etc. Finally, as such, AmI-HSs themselves are considered as medical devices since, according to the article 1,(2)a of the European Medical Device Directive [5], a medical device (MD) is any apparatus, along with the software with which it is equipped, used to support human activities for the purpose of diagnosis, prevention, monitoring, treatment of disease, compensation for an injury, investigation of a physiological process.

All these features heavily affect the design and development of AmI-HS and have to be taken into account from the outset. Furthermore, the last point constraints manufacturers to follow some standards for the development of MDs (e.g. IEC 62304) since such products are subject to pass through a regulatory process that certifies their quality based on the safety of users. Generally speaking, medical regulations define a risk-based certification process whose aim is to collect, evaluate and check the objective evidences useful to prove that the MD under scrutiny either prevents or appropriately mitigates all the risks users may face by using it. Neither regulations nor standards define how to produce the objective evidences specific for a particular MD.

In this paper we want to present a quantitative methodology whose aim is to fill this gap. In detail, we define a probabilistic risk model (PRM), based on Markov Decision Process (MDP), for the purpose of performing risk assessment appropriately to AmI-HSs. Particularly, our risk model considers two important characteristics of AmI-HSs, i.e. context awareness and personalisation. The former refers to the contextual and situational information an AmI-HS needs for supporting users activities. The latter concerns the presence of doctors, caregivers, nurses, patients, each one with their own roles and capabilities which have to be taken into account to evaluate and manage risks. We will apply our approach to a case study of an AmI-HS for a Nuclear Medicine department in order to show the effectiveness of the methodology proposed.

To sum up, the main contributions of this work are the following:

- the definition of a quantitative risk analysis methodology, based on probabilistic model checking (PMC) techniques, to support the AmI-HS quality assessment for the purpose of user safety.
- the definition of a probabilistic risk model to assess risk of context-aware hazard scenarios.

The remainder of the paper is structured as follows. Section 2 introduces (Subsection 2.1) the case study we use as a reference throughout the paper, then (Subsection 3) it is presented the methodology we propose. Section 3 reports the definition of the probabilistic risk model we have conceived specifically for AmI-HS. In Section 4 the case study is recalled to show an application of our methodology and its feasibility. Section 5 presents a brief description of related work. Finally, Section 6 concludes the paper and discusses future directions.

2. The Dynamic Probabilistic Risk Assessment Methodology

2.1. Case Study

The case study we present is taken by [3]. It is an application of Ambient Intelligence to a department of Nuclear Medicine (AmI-NM). Within the NM department the patients who need to be examined have to take specific radiopharmaceutical, i.e. a radioactive agent, according to the diagnostic imaging examinations to be performed (e.g., blood volume study, bone scan, brain scan, etc.). Once such agent is taken, the patients emit radiation and have to stay in a specific room to wait for until the radioactive agent passes through, or is taken up by, the organs to be diagnosed. The time the patients have to wait depends on the kind of examination to be performed and the time that the radiopharmaceutical takes to propagate within the body so as to reach the right radioactive level. In fact, examinations can be carried out only if the radiation level is within a certain range. After the patient's examination, he/she goes to the waiting room until the level of radiation he/she is emitting falls below a specific threshold and so becomes harmless.

Currently, the patients are accompanied by nurses when moving within the department. The goal of the AmI-NM is to have an automatic system that would guide patients within the department and so free specialised medical staff. Thus, the system has to ensure that patients strictly follow the medical procedure. For this reason, it has to be able to track patients movements in the department, and to monitor their heart rate as well as their radioactive level so as to promptly send alarms to caregivers if something wrong happens (e.g. possible undesired effects due to the injection, the stay of a patient in an area either forbidden or radioactive, the change of the diagnostic procedure because of some unforeseen circumstances).

For our purpose we abstract away from a specific NM department and then we consider it as being constituted of four locations:

1. the Acceptance Room (AR), which is the room where the patients are accepted into the department to wait for their injection.
2. the Injection Room (IR), which is the room where the patients receive the injection.
3. the Waiting Room (WR), which is the room where the patients wait for the examination after having been injected and until the radiation level reaches the correct range.
4. the Diagnostic Room (DR), which is the room where examinations are performed.

The last three rooms are equipped with short-range RFID readers so that patients can be tracked by the system. Within the AR, an operator registers the patients and equips them with an RFID tag, an ECG sensor, a radiation dosimeter, and a Personal Digital Assistant (PDA). After the registration phase, the system receives data streams from these sensors in such a way it can monitors, controls, and manages patient's activities and environmental conditions.

When the patient moves into an area, the system determines the presence of a new RFID tag in a physical location by means of the RFID reader. For instance, an event like Tag = 127; RFID Reader = 2 is produced and translated into semantic information (e.g., Patient = Massimo Rossi; Location = Injection Room). For the sake of brevity we refer readers to [3] for further information about the system design and architecture.

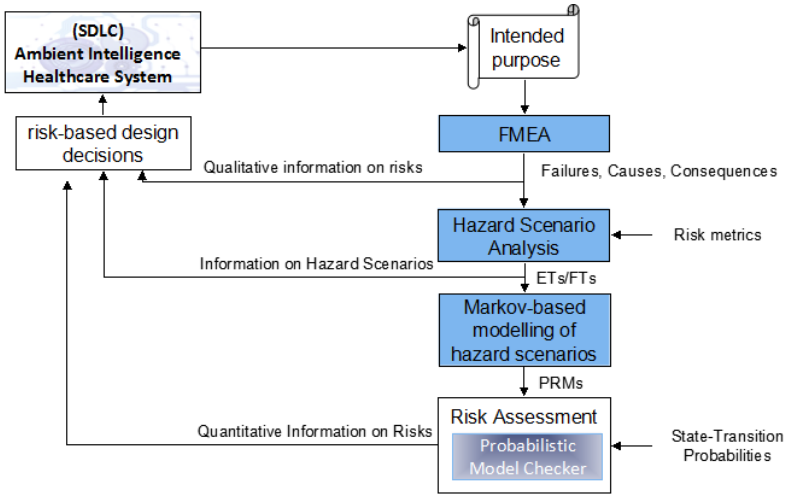

Figure 1. Dynamic Probabilistic Risk Assessment methodology based on Markov Chain Model Checking

2.2. Risk-based Approach

Risk Analysis (RA) and Management is of utmost importance for the MD software industry since it is the means by which assuring that unacceptable risks are avoided and acceptable ones are mitigated for the safety of both patients and healthcare operators.

For the nature of AmI-HSs, the state of the art RA method known as Failure Mode and Effects Analysis (FMEA) [6] is limited due to its subjective and semi-quantitative estimation of risk severity and probability ranking, but far more because it does not take into account the dynamics through which a negative consequence results from a hazard event (failure).

The methodology we have conceived is based on the Dynamic Probabilistic Risk Assessment (DPRA) [7] approach which overcomes the aforementioned issues related to a traditional static method (see [8]). Widespread DPRA formalisms such as Event-Tree (ET) [9] and Fault-Tree (FT) [10] are particular useful to represent and analyse hazard scenarios of systems with the following characteristics:

- The system's responses and/or results are influenced by the dynamics of phenomena
- The process dynamics affect the behaviour of hardware/software component failure, the human operator actions, and the human-machine interactions.
- Some failure modes are related to the process dynamics.

To address the complexity of AmI-HS and to take into account both the human factor and the context awareness, the ET/FT solution is limiting because the event order is fixed for a hazard scenario, the temporal aspect is not considered, and it is not possible to account for context-dependent events.

To account for such aspect we define (see Section 3) a Markov-based probabilistic risk model (PRM) as a formal model to represent hazard scenarios. A probabilistic model checking (PMC) technique [11] is then exploited as an automatic, efficient, and powerful solution to perform both qualitative and quantitative risk assessment.

The methodology we propose is illustrated in Fig. 1. It still takes advantage of both FMEA and ET/FT techniques to, respectively, obtain risk information with respect to the static elements designed into the AmI-HS (through qualitative and/or semi-quantitative analysis) and also the dynamics of hazard scenarios.

Particularly, during the Software Development Life Cycle (SDLC) of an AmI-HS from the intended purpose document, an FMEA is carried out to identify hazards, their causes, and consequences, as well as to prioritise hazards on the basis of their effects on the system users. For those hazards that needs to be examined in more detail, the "Hazard Scenario Analysis" phase allows the disclosure of the actual dynamics which relate causes and effects. The results of such a phase is a set of ETs/FTs describing the hazard scenarios of interest. The last two phases are the real innovation of this methodology. The input of the "Markov-based modelling" phase is the output of the previous phase, i.e. the set of ETs/FTs. These serve in supporting the definition of the PRMs representing the scenarios which must be analysed.

Finally, to perform risk assessment of hazard scenarios, the PRMs are implemented and analysed by using the probabilistic model checking tool PRISM [12]. Specifically, the PRMs can be described in a parameterised way with respect to transition probabilities. In this way, by tuning the model parameters, i.e. the transition probabilities, it is possible to quantify the total risk for different realisations of the same scenario so to both better support the risk analysis process and take into account the unavoidable uncertainties that experts' estimations or real measurements of probabilities bring in the assessment phase. Choosing or estimating transition probabilities is not within the scope of this paper, but references (such as [13,14]) are given in the literature .

3. Probabilistic Risk Model

In the following we present the probabilistic risk model (PRM) conceived within the methodology we proposed in Section 2 As a starting point we have taken the formal definition of generic AmI systems given in [2]. In that work, an AmI system is defined as being composed of three main items: a real environment, and a set of interaction constraints, a set of occupants, e.g. humans, pets, robots, etc.

Our insight for defining a PRM derives from focusing on the following important aspects related to risk in the fields of both Medical Devices and AmI:

- take into account those interaction constraints in which hazards for intended users can be present
- formalise those interaction rules for which the AmI system decision-making process for supporting human activities may experience failures
- consider each category of human and non-human occupants that are involved in hazard scenarios
- model the physical spaces within the whole environment - hereafter we call them contexts, in which events of interest for evaluating hazard situations may be generated
- represent only those human actions that contribute in some way to hazard situations

For the last point it is worth emphasising that the set of human actions vary according to the type of people as well as to the space in which occupants are immersed. For

instance, as we will see in the example presented in Section 4, in our reference case study patients or caregivers act differently if they are in the injection room compared with the diagnostic room.

We thus formally define a PRM for an AmI-HS as follows:

$$PRM = \langle C, O, \{MC_i\} \rangle$$

where:

C : is the state space, i.e. the set of contexts making up the environment in which the AmI-HS gives support to human activities. To the purpose of analysing hazard scenarios, we augment such space with two virtual contexts "Not Allowable" and "Unknown" which aggregate, respectively, all the other contexts in which an occupant should not be and the possibility that the system fails to determine the context in which an occupant is.

O : is the set of occupants[2] denoted by $O = \{1, \ldots, n\}$

MC_i : is what we define a Context Markov Decision Process (Ctx-MDP) for each occupant $i \in O$, i.e. an MDP which allows us to model both the behavioural movements and the possible sequences of actions performed across and within contexts by an occupant

In detail we define a Ctx-MDP MC_i for an occupant $i \in O$ as an extension of a MDP in the following way:

$$MC_i = \langle \{m_c\}, Act, P, R \rangle$$

in which:

$\{m_c\}$: is the MDP modelling the stochastic and non-deterministic behaviour of the occupant i within the context $c \in C$.

Act : is the set of actions, composed of {`move-in, move-out`}, which allow modelling of when an occupant comes into or moves out of a context.

P : is the probability distribution that captures the stochastic aspect of an agent's behaviour. It is defined upon the transition function $T : C \times Act \times C \to [0,1]$.

R : is the reward function $R : C \times Act \to \mathbb{R}$ which, given a context $c \in C$ and an action $a \in Act$, specifies a real number. In particular, we assume positive numbers are rewards, whereas negative ones are costs.

Intuitively, a Ctx-MDP is an MDP which models the stochastic behavioural movements of an occupant within the environment, partitioned in the set of contexts C. Moreover, for each $c \in C$, m_c is the MDP which represents the behaviour an occupant exhibits when he/she is within that context.

[2] without loss of generality, an occupant $i \in O$ can represent either a single person or a category of people, e.g. patients having the same pathology

Failure	Cause	Consequence
Contrast agent has passed its peak in the patient's body	accelerated heart rate	Patient fails to follow the examination procedure

Table 1. Failure Case from FMEA

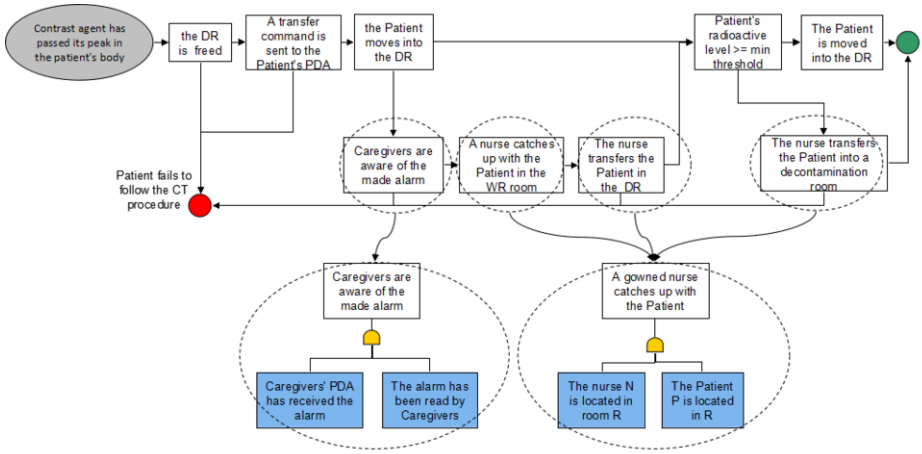

Figure 2. Dynamic Probabilistic Risk Assessment methodology Example

4. Preliminary Experiment and Results

To validate the feasibility of our PRM and DPRA methodology, in the following we present a preliminary experiment conducted on the case study described in Section 2.1.

For the sake of brevity, we will focus our attention on the last two stages of our methodology with respect to the instantiation of the PRM and its evaluation by means of the probabilistic model checker PRISM[12]. We refer readers to our previous work [8] to see a practical application of our approach in the generic context of Medical Devices.

With regard to the AmI-HS for a nuclear medicine (NM) department, we choose to analyse the failure case shown in table 1 and taken as a results of an FMEA. It is straightforward to infer that such situation can only happen subsequently to when the radioactive agent has been administered to the patient. What is not inferable is where the patient could be located when this hazard event occurs. In fact, the probability of the patient failing to following his/her examination procedure may change if, for instance, the patient is still in the WR rather than being in the DR and ready for examination. The AmI-HS of our case study deals with automatising and managing the examination procedure within the NM department. Therefore, we assume that by means of the dosimeter sensor, the system knows when to send a command to the patient's PDA that suggest to him/her to move onto the DR for examination. An FMEA is not sufficient to analyse the dynamics of such situation, hence this is where, by using the ET/FT formalism, a DPRA approach is of great benefit.

Fig. 2 shows a hazard scenario in which an ET/FT analysis helps in identifying the sequences of events that from the occurrence of the hazard state leads to success/unsuccess end states.

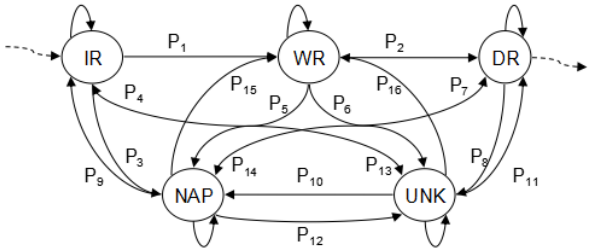

Figure 3. Context-MDP for patients

As it is clear, the ET scenario abstracts away from the spatial aspect related to where patients and caregivers are located. Such information differentiates various scenarios all having as a reference model that pictured in Fig. 2. A hazard scenario is then a means which drives the construction of the associated PRM.

In [8] we have already proposed how a hazard scenario can be mapped into a pure Markov Decision Process (MDP) risk model and, also, we have discussed the advantages in using an MDP model such as the introduction of the temporal aspect, and the capability of representing more complex scenarios due to the presence of loops and arbitrary reward functions on states and transitions. In this work we have defined a PRM based on an MDP extension we call Context MDP, or Cxt-MDP for short. Fig. 3 shows the Cxt-MDP which captures the behavioural movements of patients in the NM department case study. The states IR, WR, and DR represent the three rooms within the MN department. The two states ”NA” and ”UNK” model the fictitious spaces ”Not Allowable” and ”Unknown”, respectively. The former allows us to take into account the cases in which an AmI-HS user either is within a not permitted area or is not in the area expected by the specific medical procedures encoded into the system. The latter considers all cases in which the AmI-HS is not able to determine the user's position within the department. This Ctx-MDP can be easily instantiated and adapted to model the stochastic process of moving from one place to another for each category of occupants. Moreover, our PRM allows us to also model the occupant's behaviour according to each context taken into account. In doing so we are able to minimise the model complexity with respect to the case in which a unique MDP is used. In our case study, for instance, the operator that receives patients in the AR is qualified to register them and to provide them with their RFID bracelet, whereas a nurse located in the IR is in charge of administrating the radiopharmaceutical to patients. Therefore, we can “personalise” the model by representing what is really needed for the purpose of risk assessment.

To model the hazard scenario of Fig. 2, we consider only two categories of occupants, i.e. caregivers and patients, and the three contexts of the IR, WR, and DR. To build a PRM we can abstract away details not needed to compute the risk. Thus, we choose to model the caregivers' states by considering not the real actions they can perform but rather the effects such actions have on the caregivers in terms of their availability to be engaged in corrective actions for mitigating risks. As a consequence, we model the caregivers' MDP with three states: Available (AV), Interruptable (INT), Uninterruptable (UNINT). To simplify the whole PRM, we instantiate this MDP for every context. We only adapt the transition probabilities according to the usual behaviour caregivers exhibit with respect to the activities they carry out in that context. As for the patients' model,

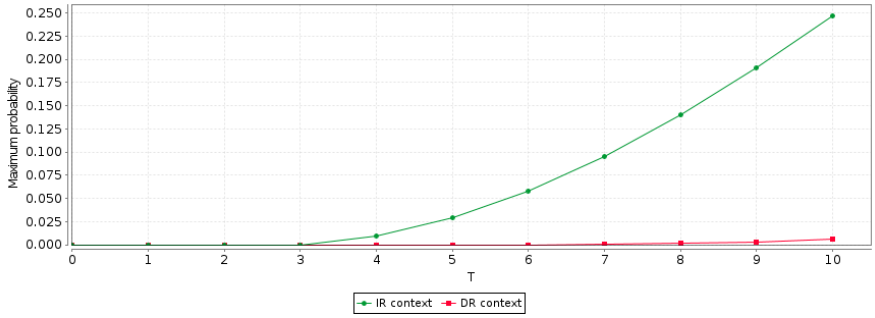

Figure 4. Probability of reaching a hazard state in either the IR or DR context

we differentiate it with respect to the context IR, WR, and DR. In all we consider to model the radioactivity level according to whether it is increasing (INC), in the appropriate range for examination (READY), out of range but not below a safe threshold (OFR), or of a safe level and decreasing(SLAD). In addition, in the IR context we also encode the states denoting whether the injection has been executed (INJ) or not (NOTINJ), by which in turn it is determined if the patient can leave the IR to move on into the WR.

We have realised our PRM by mapping it into a parallel composition of reactive modules[15] described and processed by the PRISM model checker. We want to warn the readers that the evaluations are obtained with respect to a stochastic model whose transition probability distribution does not represent actual measures taken by real situations of a nuclear medicine department.

Fig. 4 shows the probability, we denote P_c, that a hazard end state (which represents the occurrence of its negative consequences) is reached, given that the failure shown in table 1 happens. The Probability Computation Tree Logic [11] is the formal language used to express properties related to MDPs. In our case to compute P_c we define in the PRISM language the following expression `Pmax=?[F<=T "viol_state" AND "viol_ctx"]` which intuitively means "what is the maximum probability of reaching the state `viol_state` (negative consequence) of the context `viol_ctx` within T time units?" The graphs of Fig. 4 plots the value of P_c by considering for `viol_ctx` with respect to both the IR (green line) and DR (red line) contexts, respectively. In the model we take into account the delay between the time wherein a decision regards a human-based command is taken by the system and when it is actually performed by humans, i.e. in this case the patient moves on towards the DR. In fact, the picture shows a zero probability in the first time units in both graphs. Then P_c increases more in case when the patient stays in IR than when in DR because in this latter case the patient is already in the room where the examination can be promptly performed without waiting any longer.

5. Related Work

As far as in our knowledge only Grunke et. al in [16] define a Risk Analysis approach which combines a probabilistic model checking (PMC) technique with a traditional Failure Mode and Effects Analysis (FMEA). Particularly, in the broadest context of system safety the authors define a probabilistic FMEA, they call pFMEA, by using a Continuous-Time Markov Chain (CTMC) as a model for formally specifying the system and its in-

teractions with the environment. As such, their focus is on analysing a stochastic failure model of system components, and the FMEA is used as a risk analysis technique to mainly identify and relate system components and failures.

In contrast, the methodology we presented is based on a Dynamic Probabilistic Risk Assessment approach which focuses on formally specifying risk scenarios and performing quantitative evaluation of risks in the specific context of Ambient Intelligence Heathcare Systems (AmI-HS). In detail, we defined a formal probabilistic risk model (PRM), based on a Markov Decision Process (MDP), to capture two important aspects of such systems, i.e. the context-awareness and the human factor. We also exploit a Probabilistic Model Checking (PMC) technique as a means to both specify the PRM and conduct risk assessment. We emphasise that our attention is on risk scenarios centred on the safety of patients and medical staff, thus considering not only the system itself, but also human actions, event concurrency, and non-deterministic situations.

Other works [1,17,18] in the context of AmI systems are more focused on verification and validation techniques and, as such, the approach is system-centred and not human-centred. Verification techniques presented by Augusto, and McCullagh [1] are based on modelling the behaviour of each device composing the AmI system as an automaton. In particular the authors discuss the use of timed automata and then the verification of behavioural properties written in Timed Computation Tree Logic to be checked by using a model checker. They also use temporal properties and finite state automata to, respectively, specify the properties and model the devices of an Intelligent Domotic Environment (IDE) system in order to verify its functional correctness.

Muñoz et al. [17] address the problem of AmI system security and dependability by focusing on a formal description and automatic verification of all possible interactions which may arise among system components. Specifically, the authors' research aims at studying and analysing the use of the AVISPA (Automated Validation of Internet Security Protocols and Applications) model checker to model and validate protocols in AmI environments. Neither the human factor nor the context-awareness are taken into account.

In [18] a design-time methodology is proposed to formally verify IDEs. The approach is based on using UML 2.0 State Charts as a formalism to model the behaviour of devices, the network, and the algorithms which control the system; the model is then verified against some logical properties expressed in UML computation tree logic (UCTL) by exploiting the UML Model Checker (UMC).

6. Conclusion and Future Work

In this paper, we have described a Dynamic Probabilistic Risk Assessment (DPRA) methodology which better addresses the problem of identifying and evaluating hazard scenarios for those Ambient Intelligence Healthcare Systems (AmI-HS), which are considered as Medical Devices (MDs), i.e. systems subject to an extensive regulatory process. Our approach takes advantage of traditional risk analysis and assessment techniques such as Failure Mode and Effects Analysis (FMEA) and and Event Tree/Fault Tree Analysis (ETA/FTA). The former useful for identifying hazards, whereas the latter to capture the dynamics of hazard scenarios, i.e. the sequence of events and actions which give a representation of how the system can manage problematic situations as a consequence

of an occurred failure. Hazard scenarios are then encoded into a formal probabilistic risk model (PRM) we defined in this work and on which we concentrated our attention. Particularly, the PRM extends a Markov Decision Process (MDP) in order to capture two distinctive characteristics AmI-HSs exhibit: context-awareness and personalisation.

We applied the proposed methodology to a case study of an AmI-HS for a Nuclear Medicine department. In using a PRM we shown how risk can change with respect to both in which physical place the hazard happens and which are the actual conditions of all the occupants to be taken into account in the hazard scenario. A model for this case study has been defined and the risk assessed by exploiting the probabilistic model checker PRISM as a powerful tool both to implement the PRM and to assess the risk. As a result, our methodology seems to be promising in supporting risk analysis and management for AmI-HSs.

There are some aspects which we would like to consider as future work. As for the methodology, investigating the interaction among multiple scenarios is a first research activity we would like to conduct for consolidating the safety evaluation of AmI-HSs. For this purpose, an interesting point we are going to investigate is the automatic generation of variants of risk scenarios by appropriately combining those identified as fundamental ones. A further issue concerns the severity factor which usually is considered dependent only on the final consequences of hazards, without taking into account other variables of interest. As a first step, we would consider the two dimensions treated in this work, i.e. the spatial and the human ones. With regards to our PRM, it could be of great benefit to implement a tool by which a PRM can be formalised and analysed directly so as to allow us to conduct a stronger and deeper campaign of experiments.

Acknowledgements

The research work reported in this paper has been partially supported by the eAsy inteLligent service Platform for Healthy Ageing (ALPHA) Project. The authors would like to thank the anonymous reviewers for their valuable feedback and comments.

References

[1] J. C. Augusto, P. McCullagh: Ambient intelligence: Concepts and application, *Computer Science and Information Systems* **4** (1) (2007), 1–27.

[2] J. C. Augusto: Past, present and future of ambient intelligence and smart environments, *Agents and Artificial Intelligence* (2010), Springer Berlin Heidelberg, 3–15.

[3] A. Coronato: Uranus: A middleware architecture for dependable AAL and vital signs monitoring applications, *Sensors* **12** (3) (2012), 3145–3161.

[4] G. Acampora, D. J. Cook, P. Rashidi, A. V. Vasilakos: A survey on ambient intelligence in healthcare, *Proceedings of the IEEE* **101** (12) (2013), 2470–2494.

[5] European Medical Device Directive 93/42/eec. Available at `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF`.

[6] T. Cichocki, J. Grski: Failure mode and effect analysis for safety-critical systems with software components, *Computer Safety, Reliability and Security* (2000), 382–394.

[7] S. Swaminathan, C. Smidts: The event sequence diagram framework for dynamic probabilistic risk assessment, *Reliability Engineering and System Safety* **63** (1) (1999), 73–90.

[8] G. Cicotti, A. Coronato: Towards a Probabilistic Model Checking-based Approach for Medical Device Risk Assessment, *Tenth IEEE International Symposium on Medical Measurements and Applications (in press)* (2015).

[9] J. D. Andrews, S. J. Dunnett: Event-tree analysis using binary decision diagrams, *IEEE Transactions on Reliability* **49** (2) (2000), 230–238.
[10] T. Yuge, S. Yanagi: Quantitative analysis of a fault tree with priority AND gates, *Reliability Engineering and System Safety* **93** (11) (2008), 1577–1583.
[11] M. Kwiatkowska, G. Norman, D. Parker: Stochastic model checking, *Formal methods for performance evaluation* (2007), Springer Berlin Heidelberg, 220–270.
[12] M. Kwiatkowska, G. Norman, D. Parker: PRISM 4.0: Verification of probabilistic real-time systems, *23rd International Conference on Computer Aided Verification* (2011), Springer Berlin Heidelberg, 585–591.
[13] B. A. Craig, P.S. Peter: Estimation of the transition matrix of a discretetime Markov chain, *Health economics* **11** (1) (2002), 33–42.
[14] N. J. Welton, A.E. Ades: Estimation of Markov chain transition probabilities and rates from fully and partially observed data: uncertainty propagation, evidence synthesis, and model calibration, *Medical Decision Making* **25** (6) (2005), 633–645.
[15] R. Alur, T. A. Henzinger: Reactive modules, *Formal Methods in System Design* **15** (1) (1999), 7–48.
[16] L. Grunske, R. Colvin, K. Winter: Probabilistic model-checking support for FMEA, *Fourth IEEE International Conference on the Quantitative Evaluation of Systems* (2007), 119–128.
[17] A. Munoz, A. Mana, D. Serrano: AVISPA in the validation of Ambient Intelligence Scenarios, *ARES'09 IEEE International Conference on Availability, Reliability and Security* (2009), 420–426.
[18] F. Corno, M. Sanaullah: Design time methodology for the formal verification of intelligent domotic environments, in *Ambient Intelligence-Software and Applications* (2011), Springer Berlin Heidelberg, 9–16.