Model checking the properties of ISO/IEEE 11073-20601

Goga, Nicolae; Vasilateanu, Andrei; Zhong, Daidi; Duan, Xiaolian

Published in:
2017 IEEE International Symposium on Systems Engineering, ISSE 2017 - Proceedings

DOI:
10.1109/SysEng.2017.8088268

Publication date:
2017

Model checking the properties of ISO/IEEE 11073-20601:2016 standard-based communication protocol for personal health device

Nicolae Goga[1,2], Andrei Vasilateanu[1], Daidi Zhong[3], Xiaolian Duan[4]
[1]Molecular Dynamics Group
University of Groningen
Groningen, The Netherlands
[2]Department of Engineering in Foreign Languages
University Politehnica Bucuresti
Bucuresti, Romania
[3]Bioengineering College
[4]Chongqing Academy of Science & Technology
Chongqing University
Chongqing, P.R.China
n.goga@rug.nl, andrei.vasilateanu@upb.ro, daidi.zhong@ieee.org, dxl@cast.gov.cn

***Abstract*— Engineering of medical informatics systems is a complex work because it is at the intersection of several critical domains, among which medicine, computer science, electrical engineering to mention just a few. One critical aspect of such systems is the interoperability of the different components. One key solution for the interoperability is the creation of good standards that will assure the interchange of data between products of several vendors and domains – medical devices, medical information systems, medical data, etc. In this paper a formal analysis of the ISO/IEEE 11073 -20601: 2016 Draft Standard for Health informatics - Personal health device communication - Application profile - Optimized exchange protocol is described. This family of standards specifies the communication between devices that can be agents (weighing scales, spirometers) which measure health related data and managers (laptop, smartphone etc.) that collect the information and can display or forward it. First the protocol was modeled in Promela and then the model was checked manually and also using the Spin tool that performed an automated check. The results revealed issues which can cause deadlocks. However, these issues appeared in exceptional workflows, the normal flow being designed well. This highlights the methodology of developing such protocols: concentration on normal, intended behaviors without dealing with exceptional behaviors. Using formal models can reveal problems with exceptional behaviors. The results and proposed solutions were reported to the IEEE 1073 working group and will be integrated in the standard.**

Keywords—medical standard, formal model

I. INTRODUCTION

One of the domains for which standardization efforts are needed is the domain of medical informatics systems. Such systems are complex and difficult to design and implement as cross-domain expertise is needed from critical domains among which medicine, computer science or electrical engineering.

A factor for their complexity is the requirement of interoperability of the different components. One key solution for the interoperability is the creation of good standards that will assure the interchange of data between products of several vendors and domains – medical devices, medical information systems, medical data, etc.

The purpose of this paper is to analyze a protocol standard from the ISO/IEEE 11073 family of standards for device communication. This family of standards specifies the communication between devices that can be agents (weighing scales, spirometers) which measure health related data and managers (laptop, smartphone etc.) that collect the information and can display or forward it. The service providers can leverage the ISO/IEEE 11073-PHD standards to deliver remote personal disease management services. The semantic interoperability these standards provide helps to optimize the quality and cost of such system [9].

The common framework used for establishing logical connections between systems, for making available presentation capabilities and services is described in *ISO/IEEE 11073-20601:2016 Draft Standard for Health informatics - Optimized exchange protocol* [4]. This protocol uses an abstract model for personal health data and is specialized for personal health usage.

The analysis of the protocol is done using formal methods and automated verification tools [2], based on previous work in using formal methods for the IEEE 1394.1 draft standard [5] and other standards from ISO/IEEE 11073 family [6, 7] and ISO/ANSI HL7 [8].

Authors of the article are part of this standardization ISO/IEEE 11073 group. After internal group discussions we decided to apply those techniques to *ISO/IEEE 11073-20601:2016 Draft Standard for Health informatics - Optimized exchange protocol*.

978-1-5386-3403-5/17/$31.00 ©2017 IEEE

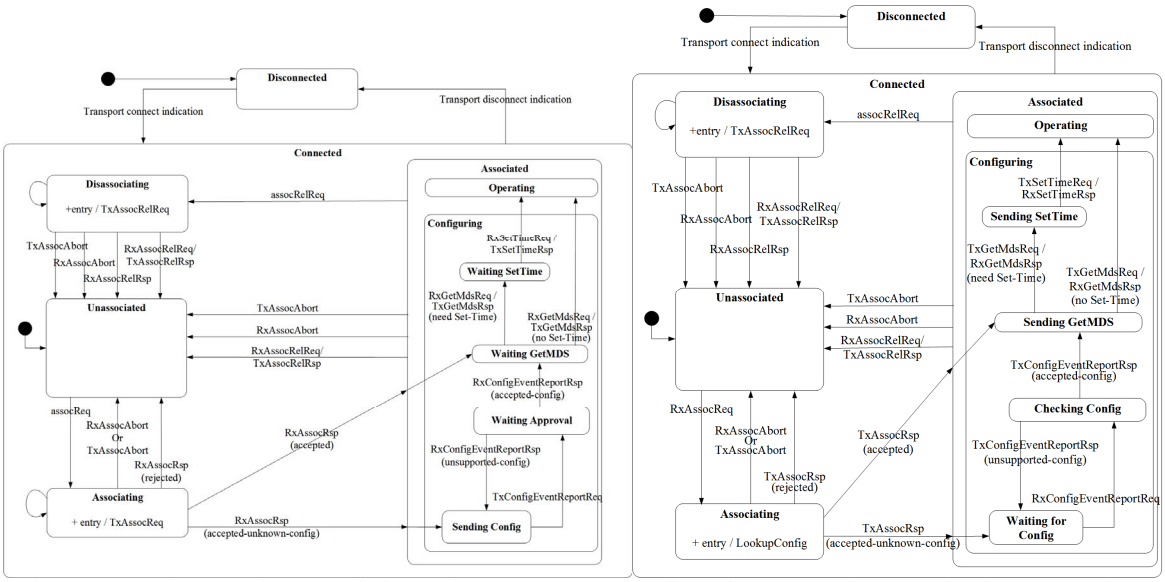

Fig. 1. The state gram of Agent and Manager device running 11073-20601 protocol. (a) The state gram for Agent. (b) The state gram for Manager

The rest of the paper is organized as follows. Section 2 gives an overview of *ISO/IEEE 11073-20601:2016* standard. In Section 3 we present the methodology applied for modeling and simulation and in Section 4 we detail the found problems and solutions. The last section details the conclusions.

II. PROTOCOL/STANDARD DESCRIPTION

In the context of ISO/IEEE 11073-PHD family of standards, the personal health devices are named as "Agent", and the counterpart is called "Manager". Typical examples of Manager devices include mobile phones, tablets and personal computers. The Agent devices typically are resource-restricted devices. Their computing power and battery power are more limited compared to the clinical device used in professional environment. The ISO/IEEE 11073-20601 standard is the baseline protocol of PHD family, which is dedicatedly designed for the personal health data exchange in such stringent scenario. It contains the following core elements:

1) *The Nomenclature* is a stable and harmonized set of terminologies of vital sign and personal health device data. It assists in use of agreed terms for the same concept to ensure semantic interoperability. The nomenclature can facilitate the efficient exchange and to ensure consistency of semantics among devices made by different vendors.
2) *The domain information model* (DIM) defines the overall set of information objects and their attributes, methods, and access functions needed for personal health device communication. This model helps Manager and Agent to reach synchronized understanding of the data supplied by Agent.
3) *The Service Model* which defines the conceptual mechanism about how the protocol interacts with objects and attributes. These services are mapped to messages that are exchanged between the Agent and Manager. As an example, the object access service contains the *GET, SET, EVENT REPORT* and *ACTION*. The measurement data is sent via the *EVENT REPORT*.
4) *The Communication Model* describes the connection state machine and details the communication characteristics. To service the general purpose, the *ISO/IEEE 11073-20601 Protocol* is designed to be portable over different type of lower layer transport, such as Universal Serial Bus (USB) and Bluetooth.

In 2014, the IEEE 11073-PHD WG has published a new edition of 11073-20601 protocols, in order to enhance its quality and capability. This has been adopted by ISO in 2016, the edition that we currently analyze. Within this edition, the Configuration and Set-Time procedure are serialized. The Manager shall invoke the GET service immediately after the accepting the device configuration of Agent. This allows the Manager to determine whether the Agent needs the time to be set. If so, the Set-Time action needs to be done before both devices entering Operating state. Correspondingly, the state transition tables are updated. This modification helps avoid the racing condition during Configuring state, which was considered as one of the major issues in some implementations of the previous edition. Agent and Manager initiate measurement data transmission. Event Reports are used to carry the measurement data.

The communication path between Agent and Manager is assumed to be a logical point-to-point connection. Generally, an Agent communicates with a single Manager at any point in time. A Manager may communicate with multiple Agents simultaneously using separate point-to -point connections. However, in this document we focus on only one manager-agent pair.

The communication protocol is started upon a connect indication that makes the manager aware of a new agent on the

network. Such a connect indication mechanism depends on lower network layers, and therefore it is not further defined in this standard. The model for this protocol is described in Fig. 1.

III. Modeling and Simulation

We made a model for communication protocol that is defined in this standard. We made the model in Promela Language and we did the verifications with Spin tooling [1, 3]. In the standard, the communication is defined between Manager and Agent and is modelled in state transition tables. The model presents the states of both Agent and Manager and how they process the event-handlers, i.e. the required behavior upon certain events, in each state. State tables in the standard consists of transitions and are usually represented in a tabular format with states on the horizontal axis, events on the vertical axis, and the behaviors in the corresponding positions (followed by a next state). The behavior can be of different types:

- Sending/reception of messages,
- State changes

We used this description as a basis of our models of these protocols because is compact and well defined. We abstract our model from the messages parameters that are related to transfer of patient-related data and (re-) configuration of the devices.

The transition tables have also events that need to be raised by an environment, such connection initiation or termination by a user, physical connections, disconnections of the agent and the manager, etc.

Spin model checking is based on closed systems. Therefore, we created two additional environment processes that model these events. The environment processes can be considered chaotic in the sense that such events may occur at any time and in any order.

A. Communication Channels

The standard is not explicit regarding the properties of the network that underlay the communication. We were particularly interested in the following aspects:

-whether the order of the messages is preserved.

-whether messages can be lost

Regarding the preservation of the order of messages, we tried to look into the standard about how to interpret absence of an event-handler for a given event in a given state. With respect to the message loss, we only assumed this to possible for a message type whenever it is explicitly mentioned in the standard.

We considered that the communication channels are not order-preserving. This assumption we made it after consulting the standard. This is in general true in networked environments, where first-in-first-out channels are not common to establish. Absence of an event-handler for a given event in a given state in the state transition tables can be interpreted as delay handling this event to a state in which it can be handled. For this we used random-receive channels of Promela

We assumed that the communication channels between the manager and the agent contain a bounded buffer. However, for the case of association abort messages, their number might be potentially unbounded. We adapted our models such that these amounts are also bounded.

IV. Results

The analysis of the aforementioned protocol is executed in two steps. In the first step, we implemented the models defined in ISO/IEEE 11073-20601 protocol and have identified some basic problems that affect the correctness of our models.

After fixing these problems, we entered the second step, where we carried out the automated test for safety-related properties, such as the deadlocks and unreachable code. Again, some issues have been identified. We fixed these issues, and the resulted models have passed the re-checking without error.

The content below summarizes our findings obtained from our analysis. We discussed them with IEEE 11073-PHD working group. Modifications typically consist of changing states to correct ones, introducing the renaming of event-handlers, etc.

A. Basic Problems

Our initial implementation, which is literally following the requirements, specified by the state transition tables in 11073-20601 standard, was somewhat hindered by the expression of message content described in those tables. The main problem is that for some concepts several long names are used. Apart from confusing us, it's not easy to find the right correspondence between the signals, especially for fresh

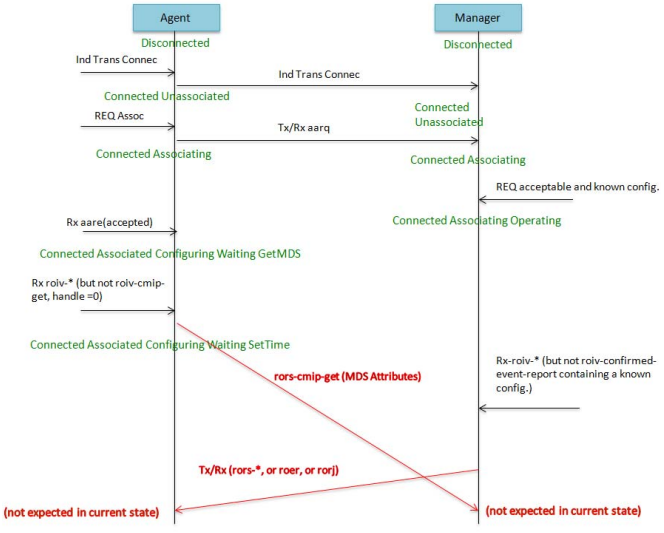

Fig 2. The Agent does not receive *Tx/Rx (rors-*, or roer, or rorj)* message in the current state and the Manager does not receive *rors-cmip-get (MDS Atrtributes)* message in the current state. They should be added or otherwise a deadlock will occur.

implementers who don't have a priori experiences on this protocol.

B. Safety Problems

We used the model-checking tool Spin to do an automated model check to identify safety gaps. The simulation was carried with Spin on an Intel i5, with the frequency of the processor of 1.3 GHz, and using the default Spin parameters.

The potential deadlocks, numbers of messages and dangling messages are the key phenomena we were concentrating on. The dangling message is a message that is not appropriately received by the receiver and hence remains in the system. It is likely to cause buffer overflow to the device. In addition, it may also cause more serious problems when such dangling message is unintentionally received somewhere after the targeting timeframe. The safety problems we found often result into the so-called unexpected behaviors, which may further lead to the deadlocks. Here we illustrate one example of such deadlock, from more possible scenarios in Figure 2.

By modified the state transition rules, we implemented the corrections in our Promela model. After that, several simulations with different random seeds have been executed. No further problem has been identified, which suggests the robustness of the refined model.

V. CONCLUSIONS

The creation of good standards is a key solution in engineering complex medical informatics systems. One critical aspect of such systems is the interoperability of the different components assuring the interchange of data between products of several vendors and domains – medical devices, medical information systems, medical data, etc.

In this paper a formal analysis of the *ISO/IEEE 11073 - 20601: 2016 Draft Standard for Health informatics - Personal health device communication - Application profile - Optimized exchange protocol* is described. First the protocol was modeled in Promela and then the model was checked manually and also using the Spin tool that performed an automated check. The results, shown in Section 4, revealed issues which can cause deadlocks. However, these issues appeared in exceptional workflows, the normal flow being designed well. This highlights the methodology of developing such protocols: concentration on normal, intended behaviors without dealing with exceptional behaviors.

In conclusion this article shows that using formal methods in designing medical informatics systems can reveal problems with exceptional behaviors which otherwise would have gone unnoticed.

The results and proposed solutions were reported to the IEEE 1073 working group and will be integrated in the standard.

ACKNOWLEDGMENT

This work has been funded by University Politehnica of Bucharest, through the "Excellence Research Grants" Program, UPB – GEX 2017.

REFERENCES

[1] G.J. Holzmann, "The Model Checker SPIN," in IEEE Transactions on Software Engineering, 23(5), 1997, pp. 279-295.

[2] E.M. Clarke, O. Grumberg and D. Peled, Model Checking, MIT Press, 1999.

[3] G.J. Holzmann, Spin -- Formal Verification, Available: www.spinroot.com [Accessed: 15 May 2017]

[4] The Institute of Electrical and Electronics Engineers, ISO/IEEE 11073-20601 Standard for Health informatics - Personal health device communication - Application profile - Optimized exchange protocol. ISO/IEEE 11073-20601.

[5] I.A. van Langevelde, J.M.T Romijn, and N. Goga. "Founding firewire bridges through promela prototyping," in 17th International Parallel and Distributed Processing Symposium (IPDPS), 8th International Workshop on Formal Methods for Parallel Programming: Theory and Applications (FMPPTA). IEEE Computer Society Press, 2003.

[6] A. J. Mooij, N. Goga,W. Wesselink, and D. Bosnacki. "An analysis of medical device communication standard IEEE 1073.2," in Communication Systems and Networks, IASTED, ACTA Press, September 2003. pp 74–79.

[7] A.J. Mooij and N. Goga. "Dealing with non-local choice in IEEE 1073.2's standard for remote control," in 4th SDL And MSC Workshop, LNCS, 2004.

[8] W. Wesselink, N. Goga, A. J. Mooij, and R Spronk. "Formal methods impact on ANSI standard HL7/im – filling gaps in msc theorys," in IEEE Canada 2005. IEEE, May 2005.

[9] Y. Li, J. Tan, B. Shi, X. Duan, D. Zhong and X. Li. "Information and Communication Technology-Powered Diabetes Self-Management Systems in China: A Study Evaluating the Features and Requirements of Apps and Patents," in JMIR Diabetes 1(1), 2016.