Published in final edited form as:
Proc IEEE Int Symp High Assur Syst Eng. 2014 January ; 2014: 247–248. doi:10.1109/HASE.2014.45.

Functional Alarms for Systems of Interoperable Medical Devices

Krishna K. Venkatasubramanian,
Dept. of Computer Science, Worcester Polytechnic Institute, Worcester, MA

Eugene Y. Vasserman,
Dept. of Computing and Info. Sciences, Kansas State University, Manhattan, KS

Oleg Sokolsky, and
Dept. of Computer and Info. Science, University of Pennsylvania, Philadelphia, PA

Insup Lee
Dept. of Computer and Info. Science, University of Pennsylvania, Philadelphia, PA

Krishna K. Venkatasubramanian: kven@wpi.edu; Eugene Y. Vasserman: eyv@ksu.edu; Oleg Sokolsky: sokolsky@cis.upenn.edu; Insup Lee: lee@cis.upenn.edu

Abstract

Alarms are essential for medical systems in order to ensure patient safety during deteriorating clinical situations and inevitable device malfunction. As medical devices are connected together to become interoperable, alarms become crucial part in making them high-assurance, in nature. Traditional alarm systems for interoperable medical devices have been patientcentric. In this paper, we introduce the need for an alarm system that focuses on the correct functionality of the interoperability architecture itself, along with several considerations and design challenges in enabling them.

I. Introduction

Recent years have seen the emergence of a vision of dynamically composable and interoperable medical devices systems. Interoperable medical devices can integrate information from multiple clinical sources in a context-sensitive way to guide patient care or prevent common critical mistakes [1]. Various agencies and standards bodies, including the U.S. Food and Drug Administration, have signaled that the future of medical technology lies in medical device interoperability [2]. Currently, devices from different manufacturers cannot communicate except in very limited ways, so even this simple level of coordination is hard to achieve without a standardized interoperability protocol. High-assurance device interoperability will be a critical requirement in realizing this vision.

Already many communication standards have been proposed, and more are in development for enabling interoperability in medical device systems. One of them is the ASTM 2951 standard called *Integrated Clinical Environment* [3], also known as MD PnP ICE. Logically, the ICE architecture is separated into Supervisor, Network Controller, and medical devices, although many components may be implemented on the same physical hardware. ICE allows coordination between each medical device through the Network Controller, a sort of “medical router” that does not have any medical/clinical functionality itself, but is

responsible for data routing, translation, and quality of service (QoS) enforcement, and generally facilitating communication between devices and the Supervisor. The Supervisor is responsible for executing "clinical workflows," from common and easily scriptable tasks such as taking blood pressure at predefined intervals and recording the results, to more complex procedures like medication interaction monitoring and suppression of likely false alarms. The clinical workflows are analogous to "apps" running on the Supervisor, which is responsible for ensuring their isolation and directing data flows from the devices (through the Network Controller) to the appropriate apps. An ICE setup is customized (usually by the appointed clinician) for each patient for whom it is deployed, in terms of the included devices and apps.

Work is already underway to build smart alarms for ICE-like architectures. These alarms focus on detecting patient health deterioration by correlating information from multiple vital sign sources [4], [5]. However, this is not sufficient for a high-assurance interoperable system. Given the complex interaction of medical devices, one needs to monitor the "health" and proper functionality of the ICE itself at run-time, in addition to reasoning about the system pre-deployment. To ensure system safety, alarms must at least continually verify that design-time assumptions hold at run-time. Ideally, given the safety-critical nature of ICE, any fault or malfunction, either natural or malicious, needs to be detected and alarm raised and addressed by clinicians, IT personnel, and/or auditors. We refer to alarms that focus on the health and wellbeing of the patient and those monitoring operation of the interoperability setup itself as **patient alarms** and **functional alarms**, respectively. From here on, *we focus on functional alarms which monitor ICE itself* rather than alarms which monitor patient health (the latter is a job for other ICE components).

II. ICE Alarm System (IAS)

The alarm subsystem of ICE must be carefully designed ahead of time in order to increase our confidence in the overall system at run-time. Alarm systems in general have two main characteristics: the *level of intelligence* in identifying alarm events and their priority with minimal delay after their occurrence, and the *alarm signal* which informs of the presence of the alarm condition through various means such as sound, vibration, or visual cues [6]. There are many different ways in which functional alarms can be built into ICE. The simplest is a *passive alarm* system that has limited in-built intelligence. It receives triggers from the Supervisor and informs clinicians through an alarm signal. Another option is to have an *active alarm* system that is intelligent and determines semi-autonomously when an alarm signal should be triggered. It is the second option that increases the ICE's assurance level.

Viewing the ICE architecture as a device monitoring the patient, we take the view of a centralized alarm subsystem, called **ICE Alarm System (IAS)**. IAS is responsible for monitoring the operation of architecture components and sounding an alarm if the operation violates specific requirements. The alarm subsystem has its own set of requirements, i.e., variables that it should monitor during the operation of ICE. Figure 1 is a design sketch of ICE incorporating such an alarm subsystem, including data flow between the components. The IAS interfaces directly with the Supervisor and gets cues from it to raise alarms,

especially those related to patient well-being. In addition, the Network Controller component mirrors all ICE traffic to the IAS. This additional information allows alarm system logic to detect problems with ICE itself without relying exclusively on other entities, which might themselves be faulty.

III. IAS Design Challenges

Most stand-alone medical devices currently come with their own alarms which are raised if the device malfunctions or reads patient data outside of pre-defined thresholds. How does one reconcile the patient alarms and functional alarms raised by the device with IAS-generated alarms? One could take two approaches in this regard. (1) Allow the devices to alarm independently, and use the ICE alarm only for problems with other components, e.g., the Supervisor, logger, Network Controller, and apps. (2) Subsume all the alarms of the medical devices, and raise all alarms in the ICE architecture centrally. This will require the interoperability data communication standards to send alarm triggers from the devices to the ICE alarm system. While centralization has its benefits, e.g., prioritization and/or suppression of false alarms, it also comes with new problems, such as situations where the centralized alarm malfunctions or alarm information is lost. A better choice may be for the alarm subsystem to observe all the entities based on traffic mirroring by the Network Controller, and independently identify alarm triggers in ICE.

Functional alarms generated by IAS have to focus not only on binary situations like presence or absence of one or more functionalities, but should also consider intermediate states such as those involving **degraded functionality**. Examples include abnormally reduced network bandwidth, and lack of regular heart-beat signals received from individual ICE components. Each of these cases might not directly affect the patient, but over time, they can render ICE unsafe. Being able to detect degraded functionality requires techniques that can decide when the functionality degradation is serious enough to have long-term consequences. This depends on the patient's health and connected ICE architecture components, and hence precomputation may not be possible. Reasoning about degraded functionality at run-time is the subject of ongoing work.

ICE is a safety-critical system and has to provide high-assurance operation. An effective alarm subsystem must be able to detect functional problems with the entities in ICE and inform the appropriate entities (clinicians, IT managers, administrators, etc.). However, this is not easy to achieve in general without making the alarm logic arbitrarily complex, such as mirroring the entire functionality of the Supervisor and Network Controller within the alarm subsystem. For example, if an app on the Supervisor does not trigger a patient alarm with the IAS when the patient's health is deteriorating, one needs to implement the same app functionality in the alarm system to be able to detect it. This underscores the inherent trade-off between what IAS should detect and the complexity of being able to correctly implement it.

Finally, even determining the scope of IAS is a challenge. The definitions of "deteriorating health" of a patient differ depending on clinical scenario specifics, rendering this difficult to detect in the general case except for simple logic, e.g., whether or not a patient's heart is

beating at all. Heart rate, blood pressure, and other seemingly “simple” parameters which signal patient health, are not as clear-cut when dealing with the full population of potential patients. Paradoxically, if the IAS itself malfunctions, it must be able to raise an alarm for itself through some alternate means. This introduces the need for a *watchdog alarm* system in IAS. The intelligence required for detecting faults with IAS is very alarm specific and may change with the design of the IAS. A watchdog alarm for IAS is essential for improving ICE’s assurance level and is the subject of ongoing work.

IV. CONCLUSIONS

In this paper we introduced the need for a functional alarm system for improving the assurance for ICE-based interoperable medical devices. We categorized the alarms in various ways based on level of built-in intelligence (passive vs. active) and operational focus (functional vs. watchdog). We then provided a list of challenges for designing the functional alarms for interoperability architectures, including reconciling multiple alarm data sources, tradeoffs between alarm subsystem intelligence and complexity, the need for watchdog alarms, and designing alarms that are flexible enough to deal with degraded functionality within ICE. Our on-going work concentrates on an IAS design that would address these challenges.

Acknowledgments

This work was partially funded by NIH grant 1U01EB012470, and NSF grants CNS-1035715, CNS- 1239324, CNS-1224007, and CNS-1239543.

References

1. Lesh K, Weininger S, Goldman J, Wilson B, Himes G. Medical device interoperability-assessing the environment. HCMDSS-MDPnP. 2007
2. Foo Kune D, Venkatasubramanian K, Vasserman E, Lee I, Kim Y. Toward a safe integrated clinical environment: a communication security perspective. MedCOMM. 2012 [Online]. Available: http://doi.acm.org/10.1145/2342536.2342540.
3. Medical devices and medical systems—essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE). 2009 ASTM F-29.21.
4. Stevens N, Giannareas AR, Kern V, Trevino AV, Fortino-Mullen M, King AL, Lee I. Smart alarms: multivariate medical alarm integration for post CABG surgery patients. IHI. 2012
5. King A, Fortino K, Stevens N, Shah S, Fortino-Mullen M, Lee I. Evaluation of a smart alarm for intensive care using clinical data. EMBC. 2012
6. Medical electrical equipment - Part 1: General requirements for basic safety and essential performance. 2012 IEC 60601.

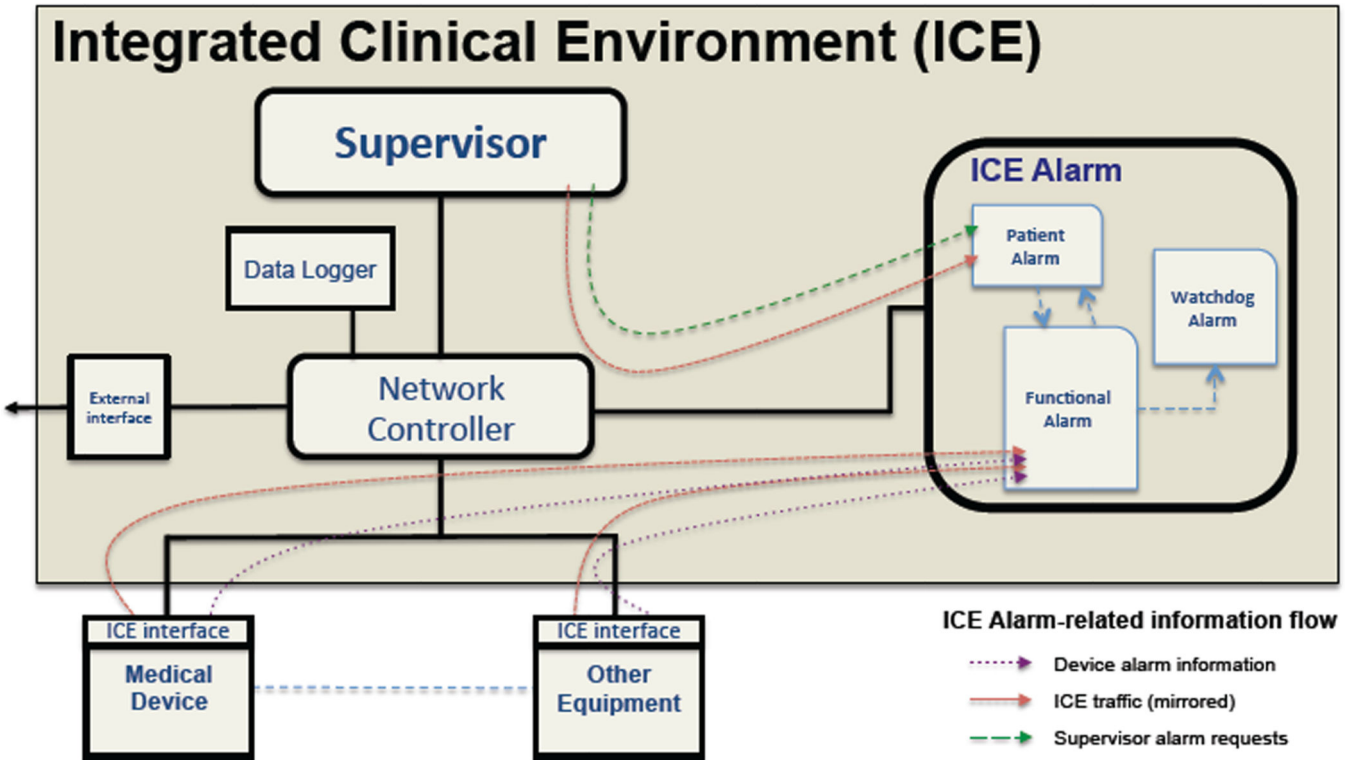

Fig. 1.

Interoperability architecture of MD PnP ICE standard, with the addition of an alarm subsystem and related data flows.