A Safety Argument Strategy for PCA Closed-Loop Systems: A Preliminary Proposal*

Lu Feng†, Andrew L. King, Sanjian Chen, Anaheed Ayoub‡, Junkil Park, Nicola Bezzo, Oleg Sokolsky, and Insup Lee

Department of Computer & Information Science, University of Pennsylvania

Abstract

The emerging network-enabled medical devices impose new challenges for the safety assurance of medical cyber-physical systems (MCPS). In this paper, we present a case study of building a high-level safety argument for a patient-controlled analgesia (PCA) closed-loop system, with the purpose of exploring potential methodologies for assuring the safety of MCPS.

1998 ACM Subject Classification D.2.9 Management (Software quality assurance), J.3 Life and Medical Sciences, K.4.1 Public Policy Issues (Computer-related health issues, Human safety)

Keywords and phrases Medical Cyber-Physical Systems, Safety Argument, Assurance Cases, Patient-Controlled Analgesia Infusion Pump, Closed-Loop Systems

Digital Object Identifier 10.4230/OASIcs.MCPS.2014.94

1 Introduction

Medical devices are increasingly used to deliver critical therapies. Because many devices are used to control the release of chemicals or energy into the patient, the safety of such devices are very important. In the United States, the Food and Drug Administration (FDA) must approve each medical device before it can be marketed. The purpose of this approval process is to ensure that each device meets an acceptable level of safety. The approval process presents challenges to all parties involved. If a company fails to obtain approval for a new device they will not be able to market it and will not be able to make a return on their investment. For the FDA considerable resources are devoted to analyzing submissions and determining if approval should be granted. Therefore, there is a need to effectively communicate and review the safety of medical device systems with a range of stakeholders (*e.g.,* medical device manufacturers and regulatory authorities). The assurance case, which is a method for expressing an argument about some properties of the system is a good way to justify the safety of medical device systems. In fact, the FDA issued a draft guidance [11] in 2010 suggesting that medical manufacturers of infusion pumps provide a safety assurance case with their pre-market submissions.

There are many challenges for both manufacturers and reviewers (*i.e.,* regulatory bodies) when it comes to effective application of the assurance case approach: for example, how can one ensure that the argument presented by an assurance case is valid (*e.g.,* logically consistent)? How can one justify the confidence of evidence used? How can one evaluate the sufficiency of an assurance case? Recently, research into assurance cases for medical

* This work is supported in part by NIH grant 1U01EB012470-01 and NSF grants CNS-1035715, IIS-1231547.

† Lu Feng is supported by James S. McDonnell Foundation 21st Century Science Initiative – Postdoctoral Program in Complexity Science/Complex Systems – Fellowship Award.

‡ Anaheed Ayoub is currently employed by Mathworks.

Medical Cyber Physical Systems – Medical Device Interoperability, Safety, and Security Assurance (MCPS'14).
Editors: Volker Turau, Marta Kwiatkowska, Rahul Mangharam, and Christoph Weyer; pp. 94–99

OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

devices has been increasing. For instance, Weinstock and Goodenough [12] discussed the safety case construction of generic infusion pumps; Jee *et al.* [4] constructed a safety case for a pacemaker; Ayoub *et al.* [2] proposed a safety pattern for model-based development, and applied it to a case study of generic Patient-Controlled Analgesic (PCA) infusion pump software.

Recent technological advancements impose additional challenges for assuring the safety of medical device systems. There is an emerging trend of network-enabled medical devices which can communicate and coordinate with each other during the treatment, forming medical cyber-physical systems (MCPS). New functionalities such as closed-loop continuous care, which was not possible with stand-alone devices, are now being developed. However, MCPS also bring new hazards (*e.g.,* network failure) to patient safety, adding more concerns for the safety argument in assurance cases.

In this paper, we consider a patient-controlled analgesia (PCA) closed-loop system, which is an example of MCPS, and build a high-level safety argument for it. The purpose of this case study is to explore potential methodologies for assuring the safety of MCPS. For the rest of the paper, we introduce the background of PCA closed-loop system in Section 2, present our safety argument in Section 3, and draw conclusions in Section 4.

2 Background: PCA Closed-Loop System

PCA infusion pumps are commonly used to deliver pain medication to patients who are experiencing high levels of pain due to serious physical trauma (*e.g.,* surgery). Patients often have different tolerance levels for pain and different reactions to the medication. Therefore, in addition to delivering opioids with a fixed schedule programmed by a caregiver, the PCA pump also allows the patient to request an additional dose of medication (called *bolus*) by pressing a button. A well-known hazard with opioid medication is that an overdose can cause respiratory failure, which may be fatal to patients [8]. There are some safety mechanisms built into modern PCA pumps. For example, a PCA pump can be programmed with limits on the number of doses it will deliver, which helps to avoid overdose no matter how often the patient pushes the bolus button. However, the existing safety mechanisms are not sufficient to protect patients in all clinical scenarios and a large number of adverse events involving PCA pumps have been reported [9]. The causes of patients receiving overdose include, but are not limited to, the following:

- the pump is misprogrammed,
- the wrong concentration of drug is loaded into the pump,
- a caregiver overestimates the maximum dose the patient can receive,
- PCA-by-proxy, *i.e.,* someone other than the patient presses the bolus button.

Obviously, there is still certain risk associated with the use of PCA pumps, to which we refer as the *residual* risk of standalone pumps.

To mitigate the overdose hazard, clinicians must monitor the patient's respiratory function through vital sign sensor readings (*e.g.,* blood oxygen saturation measured by a pulse oximeter). Then, if the patient entered respiratory distress, the caregiver would manually intervene to resucitate the patient. Unfortunately the current practice is both error prone and burdensome for the clinician [3, 5].

Recently, the notion of a "closed-loop" PCA system has been proposed to ease the burden of clinicians by interconnecting the infusion pump, pulse oximeter, and a computer controller over a network. The controller would monitor the pulse oximeter readings and, when a problem is detected, automatically stop the infusion pump and alert the clinician.

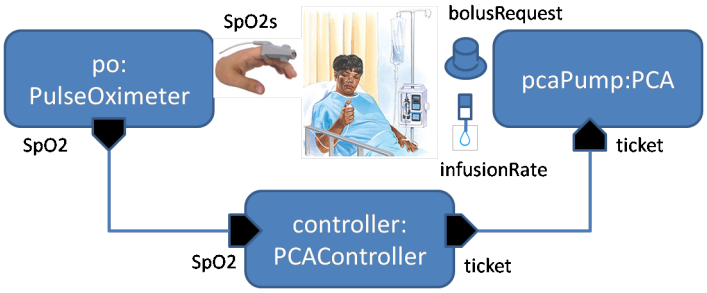

Figure 1 PCA closed-loop system overview (adapted from [7]).

Figure 1 shows the architecture and essential data flow of a PCA closed-loop system. A pulse oximeter receives physiological signals from a clip on the patient's finger and calculates the SpO_2 values (*i.e.,* the measure of blood oxygenation). The computer controller makes control decisions based on SpO_2 readings received from the pulse oximeter, and periodically issues a "ticket" to the infusion pump. Each ticket limits the bolus and basal time period that the pump can infuse before the patient could possibly be pushed into respiratory distress. If the network becomes disconnected for a long period, the pump would expire the current ticket and stop delivering pain medication to protect the patient from overdose. Unless the ticket expires or the pump is stopped by the controller, the infusion pump will continue to deliver opioids to the patient at the basal rate programmed by the caregiver. The patient may also occasionally press the button and request a bolus from the infusion pump. After the absorption of the opioid medication, the patient's respiratory state may become more depressed, which is reflected by the patient's blood oxygenation level. The safety of such a closed-loop system has been studied in [1, 10] via simulation-based analysis and formal verification.

3 Safety Argument

In this section, we develop a high-level safety argument for the PCA closed-loop system. Figure 2 shows our argument using the Goal Structuring Notation (GSN), a popular graphical notation for organizing and presenting safety argument (we refer readers who are unfamiliar with GSN to [6]).

The top-level *goal* (**G1**) is to show that "*The PCA closed-loop system is at least as safe as the stand-alone infusion pump, with respect to the overdose hazard*". Here, we assume that the closed-loop system is built on top of a stand-alone infusion pump whose safety has already been assessed in a separate safety argument, and the pulse oximeter's behavior is not affected by putting in the PCA closed-loop. This context is documented as **C1.1** in Figure 2.

To address **G1**, our strategy is to argue by risk-benefit analysis (**S1**), which is defined in the context **C1.2**. If the benefit brought by the closed-loop system outweighs its introduced risk, then we can assert that the goal **G1** is true. More specifically, the *benefit* refers to how much residual risk of the stand-alone pump can be mitigated by the closed-loop system.

Following strategy **S1**, we decompose **G1** into three sub-goals:

- **G2.1**: *The introduced risk due to hazards of closed-loop system is acceptable.*
- **G2.2**: *Some residual risk of the stand-alone infusion pump is adequately mitigated by the closed-loop system.*
- **G2.3**: *The benefit of closed-loop system outweighs its introduced risk.*

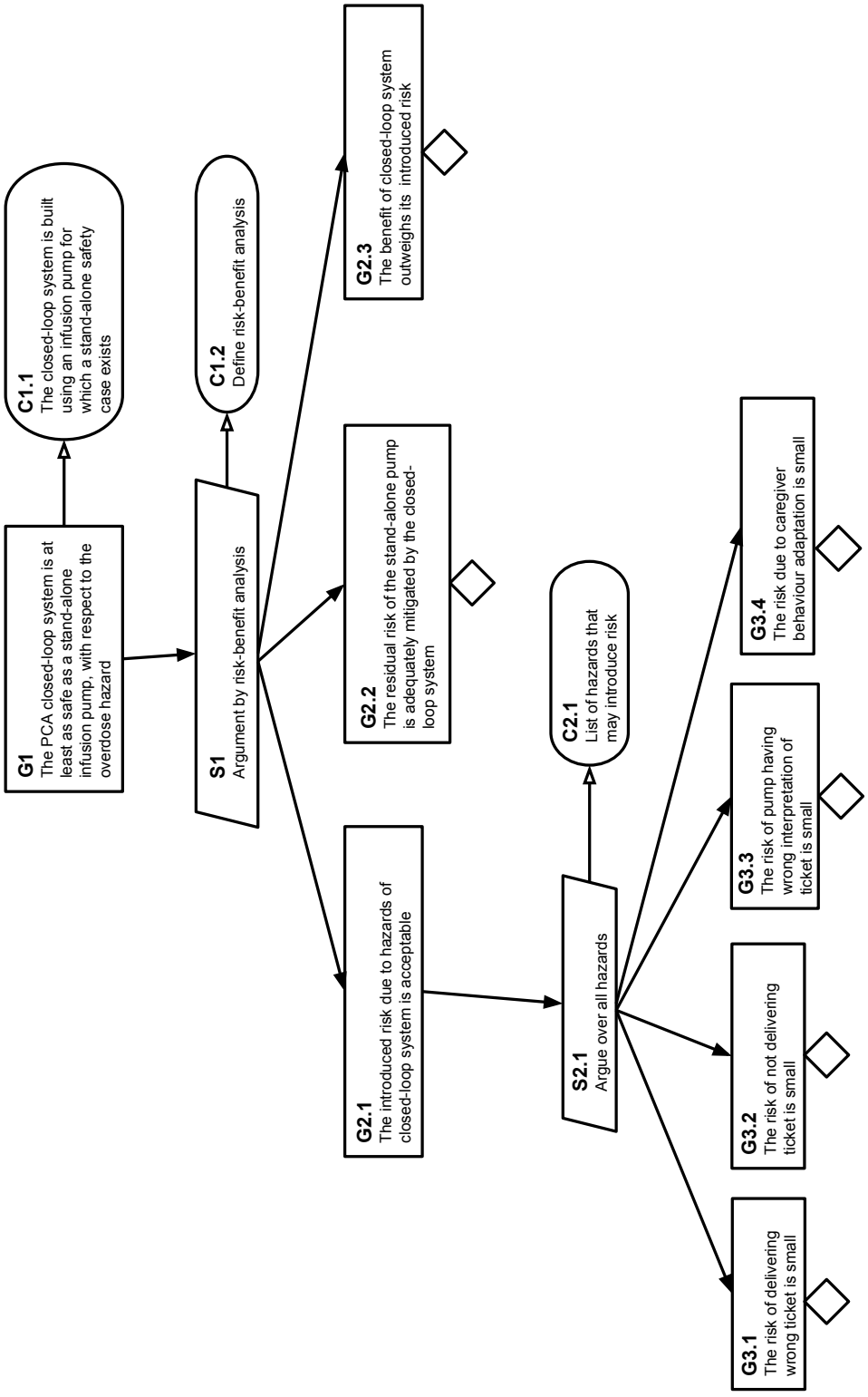

Figure 2 High-level safety argument for the PCA closed-loop system.

In Figure 2, we only further develop **G2.1** as an example, while keep **G2.2** and **G2.3** undeveloped (denoted by a *diamond* underneath the rectangle element). In the following, we elaborate on **G2.1** in more details and propose possible strategies for **G2.2** and **G2.3**.

The strategy (**S2.1**) for claiming goal **G2.1** is to argue over a list of possible hazards introduced by the closed-loop system, under the context (**C2.1**) that lists introduced hazards. This strategy leads to four sub-goals, each of which corresponds to a hazard of the closed-loop system. In Figure 2, these four goals (**G3.1-G3.4**) are not further developed. We briefly discuss their corresponding hazards as follows.

- (**G3.1**) *Delivering a wrong ticket to the infusion pump.* This hazard may be caused by incorrect controller computation, corruption of the message on the network, or incorrect sensor readings. We may argue that the risk of this hazard is small by providing formal verification evidence for the correctness of the controller algorithm. Another useful evidence is the verification of the infusion pump. If the pump correctly handles tickets arriving from the network interface, tickets cannot make the pump infuse when it would not be infusing in the stand-alone case, or infuse at a different rate. That is, at any time, the pump would be infusing at the same rate as it would be infusing in the stand-alone case, unless it has been stopped by an expired ticket. Therefore, a bad ticket would not cause more overdose than in the stand-alone case, if the pump handles the ticket correctly.
- (**G3.2**) *Not delivering a ticket to the pump.* Various reasons may cause this hazard. For example, the controller does not produce a ticket when it should, due to an incorrect implementation or incorrect sensor reading; or the calculated ticket is lost, due to disconnected network or other failures. In any case, the infusion will continue unmodified until the prescription runs out or the current ticket expires. Thus, this hazard would not introduce additional risk because the patient receives exactly the same amount of medication as in the stand-alone case.
- (**G3.3**) *The pump has a wrong interpretation of the ticket.* Recall that a ticket contains the maximum time period over which the infusion pump can infuse, a ticket that does not expire when it should due to the pump's wrong interpretation may lead to overdose. Similar to the argument for **G3.1**, we can provide the formal verification of the pump as evidence to show that the risk of hazard is small.
- (**G3.4**) *Caregiver behavior adaptation.* For example, due to the automation of closed-loop system, the caregiver may check the pump alarm state and assess the patient condition less frequently than in the stand-alone case. Or, the caregiver learns to assume that the system will self-correct and therefore applies more aggressive therapy. The argument about this hazard relies on the caregiver's training. Training materials and guidelines will be used as evidence. In additional, a sufficiently reliable new alarm system must be present to detect closed-loop system failure and notify caregivers.

We can argue goal **G2.2** in a similar way as for **G2.1**, that is, arguing over residual risk of the stand-alone pump that can be mitigated by the closed-loop system. As described in Section 2, the residual risks include, for example, the pump being misprogrammed, the wrong concentration of drug being loaded into the pump, a caregiver overestimating the maximum dose the patient can receive, or someone other than the patient pressing the bolus button. These hazards can be adequately mitigated in the closed-loop system due to the fact that, the controller would automatically monitor the patient's respiratory function via pulse oximeter readings and automatically stop the infusion pump whenever necessary to protect the patient from overdose.

Finally, goal **G2.3** takes a holistic view of benefit and risk of the closed-loop system. Essentially, we want to show that the benefit of the closed-loop system (*i.e.,* mitigating

residual risk of the stand-alone pump) outweighs its introduced risk. A formal risk-benefit analysis report can be used as evidence to support this goal.

4 Conclusions

We have presented a high-level safety argument for a patient-controlled analgesia (PCA) closed-loop system, where an infusion pump, a pulse oximeter, and a computer controller are interconnecting over a network. The goal of the argument is to show that "*The PCA closed-loop system is at least as safe as the stand-alone infusion pump, with respect to the overdose hazard*", and the strategy is to argue by risk-benefit analysis. This case study has the potential of being generalized for other network-enabled medical devices. We hope to further explore this direction in the future. Ultimately, we would like to develop a safety argument pattern for closed-loop systems.

References

1 David Arney, Miroslav Pajic, Julian M Goldman, Insup Lee, Rahul Mangharam, and Oleg Sokolsky. Toward patient safety in closed-loop medical device systems. In *Proceedings of the 1st ACM/IEEE Int'l Conf. on Cyber-Physical Systems*, pages 139–148. ACM, 2010.

2 A. Ayoub, B. Kim, I. Lee, and O. Sokolsky. A Safety Case Pattern for Model-Based Development Approach. In *NFM2012*, pages 223–243, Virginia, USA, 2012.

3 Rodney W. Hicks, Vanja Sikirica, Winnie Nelson, Jeff R. Schein, and Diane D. Cousins. Medication errors involving patient-controlled analgesia. *American Journal of Health-System Pharmacy*, 65(5):429–440, March 2008.

4 E. Jee, I. Lee, and O. Sokolsky. Assurance cases in model-driven development of the pacemaker software. In *4th International Conference on Leveraging Applications of Formal Methods, Verification, and Validation – Volume Part II*, ISoLA'10, pages 343–356, Berlin, Heidelberg, 2010. Springer-Verlag.

5 Joint Commission. Sentinel event alert issue 33: Patient controlled analgesia by proxy. `http://www.jointcommission.org/sentinelevents/sentineleventalert/`, December 2004.

6 Tim Kelly and Rob Weaver. The goal structuring notation – a safety argument notation. In *Proc. of Dependable Systems and Networks 2004 Workshop on Assurance Cases*, 2004. `http://www-users.cs.york.ac.uk/tpk/dsn2004.pdf`.

7 Andrew L. King, Lu Feng, Oleg Sokolsky, and Insup Lee. Assuring the safety of on-demand medical cyber-physical systems. In *Proceedings of the 1st IEEE International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA'13)*, 2013.

8 P. E. Macintyre. Safety and efficacy of patient-controlled analgesia. *British Journal of Anaesthesia*, 87(1):36–46, 2001.

9 Teryl K. Nuckols, Anthony G. Bower, Susan M. Paddock, Lee H. Hilborne, Peggy Wallace, Jeffrey M. Rothschild, Anne Griffin, Rollin J. Fairbanks, Beverly Carlson, Robert J. Panzer, and Robert H. Brook. Programmable infusion pumps in icus: An analysis of corresponding adverse drug events. *Journal of General Internal Medicine*, 23(1):41–45, 2008.

10 Miroslav Pajic, Rahul Mangharam, Oleg Sokolsky, David Arney, Julian M. Goldman, and Insup Lee. Model-driven safety analysis of closed-loop medical systems. *IEEE Transactions on Industrial Informatics*, 2013.

11 U.S. Food and Drug Administration, Center for Devices and Radiological Health. *Guidance for Industry and FDA Staff – Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions*, April 2010.

12 C. Weinstock and J. Goodenough. Towards an Assurance Case Practice for Medical Device. Technical report, CMU/SEI-2009-TN-018, 2009.