Acta Scientific MEDICAL SCIENCES (ISSN: 2582-0931)

Volume 7 Issue 1 January 2023

Research Article

Safety Requirements Elicitation Method for Medical Devices Using FRAM

Shuichiro Yamamoto*

Department of Information Technology, IPUT in Nagoya, Japan

***Corresponding Author:** Shuichiro Yamamoto, Department of Information Technology, IPUT in Nagoya, Japan.

DOI: 10.31080/ASMS.2022.06.1426

Received: December 05, 2022
Published: December 14, 2022

© All rights are reserved by **Shuichiro Yamamoto.**

Abstract

Background: As medical devices attached to human body shall be safe, it is important to elicit safety requirements for medical devices. So far, the risk driven approaches are used to derive safety requirements specification. We are trying to elicit safety requirements by the success conditions of medical device functions and operations which are clarified by describing the Functional Resonance Analysis Method (FRAM) diagram.

Method: Firstly, interactions of medical device functions and its human operations are described by FRAM diagram. Secondly, the success conditions of functions are identified. Finally, safety requirements of the medical device are elicited for the identified conditions.

Results: The approach is applied to elicit safety requirements of an insulin pump system. The safety requirements have been elicited by describing the FRAM diagram for the insulin pump system. The result showed the applicability of the method to elicit safety requirements.

Conclusion: The proposed approach is effective to elicit safety requirements for medical devices from the success conditions of functions identified by using FRAM.

Keywords: Safety Requirements; Medical Device; FRAM; Case Study

Abbreviations

FRAM: Functional Resonance Analysis Method; FMEA: Failure Mode Effect Analysis; STAMP: System Theoretic Accident Model and Processes; STPA: System-Theoretic Process Analysis; UCA: Unsafe Control Action; SC: Safety Constraints

Introduction

There are two approaches for analyzing safety of socio-technological systems such as healthcare services. System-Theoretic Process Analysis (STAMP) [1][2][3] analyzes safety from the point of system failure as a whole based on top-down approach. Functional Resonance Analysis Method (FRAM) [4] analyzes safety from the point of success conditions of functional activities based on bottom-up approach.

System-Theoretic Process Analysis (STPA) is proposed to analyze safety of system component interactions based on STAMP [3]. STPA analyzes the Unsafe Control Action (UCA) based on the control structure developed by STAMP. Safety Constraints (SC) is then extracted to reduce UCA.

Vilela and others [5] proposed SARSSi* (SAfety Requirements Specification method based on STAMP/STPA and i*) method to reduce the analytical gap on requirements and safety engineers. The method composes STPA hazard analysis and i* goal-oriented requirements modeling. The safety requirements are elicited from hazards identified by STAMP.

Yamaguchi and others [6] also applied STAMP/STPA to develop safety requirements of the radiation treatment system by using unsafe control actions extracted from the system control structure. The method mainly concerns safety requirements of operations between technicians and the radiation system.

The Functional Resonance Analysis Method (FRAM) analyzes functional resonance by the following steps.

- [Step 1] Identify functions.
- [Step 2] Decide functional variability
- [Step 3] Analyze functional resonance for variability
- [Step 4] Propose countermeasures against variability.

FRAM models complex socio-technical systems by using the graph consists of hexagonal function nodes and their binary relationships between aspects of nodes.

The visual icon of hexagonal FRAM node is shown in figure 1. The possible binary coupling relations of aspects are <O, I>, <O, T>, <O, C>, <O, R>, and <O, P>, where <X, Y> means X and Y are aspects of different functions.

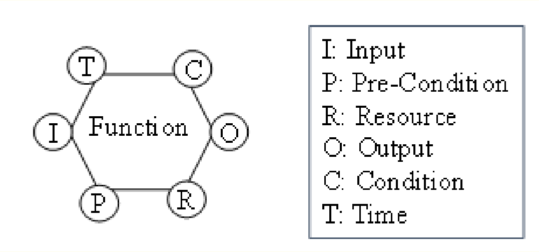

Figure 1: FRAM node.

Naeini and Nadeau [7] compared STAMP and FRAM to analyze risks in the manufacturing domain.

Several integrations of FRAM with other methods have also been proposed. Sujan and Felici [8] proposed a combination of Failure Mode Effect Analysis (FMEA) with FRAM as a complementary approach and showed it could identify vulnerabilities related to communication and handover within an emergency care.

Tresfon and others [9] showed that FRAM is very effective in comparing work-as-done with work-as-imagined, as it contributed to a better understanding, evaluation and support of everyday performance in a ward care setting.

So far, there is no safety requirements elicitation approach has been proposed using the success conditions of FRAM in the healthcare domain. In this paper, we propose a safety requirements elicitation approach by using FRAM for medical devices.

Method to elicit safety requirements using FRAM

Safety Requirements Elicitation using FRAM consists of the following four steps.

- [Step 1] Define functions of the target system for each component
- [Step 2] Define functional resonance by FRAM
- [Step 3] Define aspects of functions
- [Step 4] Elicit safety requirements according to aspects.

Result

In this study, the use case for the insulin delivery system [10] is evaluated to elicit the safety requirements by applying the proposed method.

Overview

The insulin delivery system is used for the treatment of diabetes patients in hospitals. The insulin delivery system monitors blood sugar levels and delivers an appropriate dose of insulin when required as follows [10]. The insulin delivery system uses the embedded sensor in the patient to measure some blood parameter that is proportional to the sugar level. The sensed value is then sent to the pump controller. This controller computes the sugar level and the amount of insulin that is needed. It then sends signals to the insulin pump to deliver the insulin via an attached needle to the patient. The insulin pump delivers one unit of insulin in response to a single pulse from a controller.

As the system is safety-critical, if the pump fails to operate or does not operate correctly, then the patient’s health may be damaged because their blood sugar levels are too high or too low.

System configuration

- Insulin delivery system is composed by Display, Alarm, Controller, Insulin pump, Insulin reservoir, Sugar sensor, Dosage Log memory and Battery.
- Patient care operations to manage insulin delivery are as follows.

- Patient wears sensor.
- Care taker initiates the system.
- Care taker sets upper bound of dosage.
- Care taker insert the needle to the patient.
- Care taker monitors display and alarm.
- Care taker changes battery and insulin reservoir.

FRAM diagram development

There are two types of FRAM functions, the system functions and user operations. The system functions are derived by transforming the corresponding system components. User operations are expressed as they are as FRAM functions.

Table 1 describes the functionals and its resonance relationships by lines between functions.

Function	Output	Resonate function
Wear sensor	Blood	Sense
Sense	Sugar level	Control
Control	Dosage	Record dosage
Record dosage	Dosage log	Control
Control	Dosage signal	Pump
Control	Dosage log, Error message	Display
Control	Error notification	Alarm
Pump	Insulin	Insert needle
Insert needle	Insulin	Accept dosage
Display	Dosage log, Shortage of battery/Insulin	Monitor
Monitor	Change timing	Change battery/ reservoir
Change battery	Battery	Supply power
Change reservoir	Insulin reservoir	Reserve insulin
Supply power	Electric power	Control, Alarm, Display, Pump
Reserve insulin	Insulin amount	Control
Reserve insulin	Insulin	Pump
Alarm	Error to initiate timing	Initiate
Display	Error to initiate timing	Initiate
Set upper bound	Upper bound of insulin dosage	Control

Table 1: Functional resonance relationships.

Figure 2 shows FRAM diagram of the insulin delivery system based on the above explanation. The white nodes show user operational functions. The gray nodes show functions provide by system components.

Figure 2: FRAM diagram of the insulin delivery system.

Safety requirements elicitation

Aspects for system functions are explained in table 2.

System functions	Aspect: Success conditions
Sense	P: sensor is correctly fitted to patient O: Sugar level is correctly sent
Control	I: Sugar level is correctly received I: Dosage log is correctly received T: Initiated on time R: Power is sufficiently supplied R: Insulin is sufficiently reserved C: Insulin upper bound is correctly set O: Error is notified as the input of Alarm O: Dosage log is sent as the input message of Display O: Error massage is sent to as input of Display O: Dosage signal is correctly sent as the input of Pump
Record dosage	I: Dosage log is correctly received from Control O: Dosage log is correctly sent to Control R: Memory size is sufficient to record cumulative dosage log in a day
Supply power	O: Power sufficiently supplies to Pump, Alarm, Display and Control O: Shortage of battery is notified to Control R: power is sufficiently supplied by changing battery if necessary

Pump	I: Sugar level is received correctly from Control R: Power is sufficiently supplied R: Insulin is sufficiently supplied for dose O: Insulin is correctly dosed through Needle
Display	I: Dosage log is correctly received from Control O: Dosage log is correctly displayed on time O: Error message is correctly received from Control
Alarm	I: Error notification is received from Control O: Sound an alarm on time
Reserve insulin	O: Insulin sufficiently supplies to Pump O: Shortage of insulin is notified to Control R: Insulin is sufficiently supplied by changing reservoir if necessary

Table 2: Success conditions of System functions.

As shown in table 2, the success conditions are the candidates of safety requirements of insulin delivery system.

Discussion

The proposed safety requirements elicitation approach using FRAM have been effectively applied to a medical device. By using FRAM aspects, safety requirements for device components are systematically extracted from the success conditions of functions.

Sommerville denoted the following safety requirements (SR) for the insulin pump system [10].

(SR1) The system shall not deliver a single dose of insulin that is greater than a specified maximum dose for a system user.

Although SR1 is the negative sentence form, it will be derived by combining the following success conditions of Control in table 2.

- "Dosage signal is correctly sent as the input of Pump".
- "Dosage log is correctly received".
- "Insulin upper bound is correctly set".

Sommerville also pointed the following SR.

(SR2) The system shall include a hardware diagnostic facility that shall be executed at least four times per hour.

For SR2, if the hardware diagnostic component is included in the insulin delivery system, SR2 can also be extracted by the success conditions of FRAM function "Diagnose hardware". However, "at least four times per hour" of SR2 shall be described as the Timing aspect of the function.

Since the approach uses only FRAM, it is simple and reduces learning costs. Although, we showed the application of the method only for device functions in this paper, the approach is also applicable to elicit safety requirements of user operations. For example, the success condition of the Monitor operation in figure 2 are as follows.

- I: Caretaker shall monitor the log record in display
- I: Caretaker shall monitor the error message in display
- I: Caretaker shall listen the alarm
- O: Caretaker shall change insulin reservoir if necessary
- O: Caretaker shall change battery if necessary.

In the future, it will be necessary to apply the method to other safety critical devices and quantitatively evaluate its effectiveness. We expect our approach can be applied to healthcare service as well as manufacturing domains. Moreover, it is necessary to compare effectiveness with other safety requirements elicitation methods.

Summary

The main contributions of the paper are as follows. The safety requirements elicitation method is defined by using FRAM diagrams. Moreover, it is shown that safety requirements of system components can be derived by the table to define success conditions of functional aspects. The applicability of the proposed safety requirements elicitation method has been evaluated by the case study on insulin delivery system. Although the proposed method was explained by an insulin pump system, the resulted method does not depend on the healthcare domains. Therefore, the proposed method is expected to apply in other industry domains including manufacturing.

Conclusion

We have shown that FRAM is able to elicit safety requirements by defining system functions of components with the function resonance table. Then we defined the success condition table for aspects. The safety requirements of the target system are elicited based on the success conditions. The basic idea is very simple that function is safe if it correctly works. The case study on the insulin delivery system showed the applicability and effectiveness of the proposed method. FRAM was also very useful to derive success conditions of functions. Future study includes application of the proposed method for healthcare domain as well as other industry domains and comparative study with related safety requirements elicitation approaches.

Bibliography

1. Nancy Leveson. "A New Accident Model for Engineering Safer Systems". *Safety Science* 42.4 (2004): 237-270.

2. Nancy Leveson. "Engineering a safer world: systems thinking applied to safety". *MIT Press* (2012).

3. William Young and Nancy Leveson. "Systems Thinking for Safety and Security". ACSAC 2013 (2013): 1-8.

4. Erik Hollnagel. "FRAM - the Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems". Boca Raton: CRC Press (2012).

5. Jéssyka Vilela., *et al*. "SARSSi*: a Safety Requirements Specification Method based on STAMP/STPA and i* language". In Proceedings of ANAIS DO I BRAZILIAN WORKSHOP ON LARGE-SCALE CRITICAL SYSTEMS 2019 (2019).

6. Shinichi Yamaguchi., *et al*. "Evaluation of the Application of the Safety Analysis Method "STAMP/STPA" to Requirement Development Phase". 57.5 (2018): 370-379.

7. Alimeh Mofidi Naeini and Sylvie Nadeau. "FRAM and STAMP: New Avenue for Risk Analysis in Manufacturing in the Era of Industry 4.0" (2021).

8. Mark Sujan and Massimo Felici. "Combining Failure Mode and Functional Resonance Analyses in Healthcare Settings". SAFECOMP. LNCS 7612 (2012): 364-375.

9. Jaco Tresfon., *et al*. "Aligning work-as-imagined and work-as-done using FRAM on a hospital ward: a roadmap". *BMJ Open Quality* 11(2022):e 001992.

10. Ivan Sommerville. "Software Engineering 9th edition". Addison Wesley (2011).