Extending STPA to Improve the Analysis of User Interface Software in Medical Devices

Paolo Masci[1], Yi Zhang[2], Paul Jones[2], José C. Campos

[1] INESC TEC and Universidade do Minho, Portugal
{paolo.masci,jose.c.campos}@inesctec.pt

[2] US Food and Drug Administration, USA
{yi.zhang2,paul.jones}@fda.hhs.gov

Abstract. We present a method to enhance the standard STPA causal factors categories and tailor them to the analysis of user interface software in medical devices. Our method builds on usability design principles, and aims to facilitate the analysis of specific use-related aspects of a software design that could impact the safety of a medical device. Initial evaluation of the method on realistic case studies indicates that our method facilitates the detection of latent software issues that can be hard to identify with the standard STPA categories.

1 Problem Statement

Latent design flaws and defects in user interface (UI) software often induce use errors and compromise the safety of a medical system. For example, a mobile app for diabetes management was recalled in the U.S. because its UI software erroneously reset the recommended insulin bolus dosage when the user changed the smartphone's orientation, which caused the user to inadvertently command and receive unsafe insulin therapies [4].

STPA has been proven as a powerful method for early identification of design problems in safety-critical systems, including medical devices. However, it is specialized for identifying system-level issues, but provides limited guidance to the analysis of use-related issues in complex systems.

Several extensions to STPA have been proposed to address this particular limitation of STPA. They rely on either cognitive models to capture hypotheses about human decision-making process (as in [7]), or human task models to represent the decision-making chain of socio-technical systems (as in [2]). In addition, Dokas et.al. [3] extended the STPA control model to facilitate the identification of management-level causes of use hazards.

These extensions have been shown as effective in helping developers identify unsafe control actions committed by human users. However, they still require developers to exercise experience and expertise to find answers for the key question: *What problems in the UI software design could induce the user to operate or interact with a system unsafely?*

2 A New Extension to STPA

We have developed a method for refining the standard STPA casual factor categories to facilitate the analysis of core aspects of UI software design, as well as the casual relations between UI design issues and use hazards [3].

Our method is built on usability heuristics [6] and UI design guidelines defined in medical device usability standards (ANSI/AAMI:HE75 and ISO:62366-2). It is carried out in two main steps:

1. Identify a core set of UI design principles from usability heuristics [6] and relevant usability standards.
2. Use the identified design principles to create different interpretations of the original STPA causal factors categories. Each interpretation created in Step 2 represents a new causal factors category, and embeds the knowledge about specific use-related concerns described in the considered design principle. Such knowledge provides mental scaffolding during the analysis, guiding the exploration of specific classes of UI software design issues that could impact the safety and usability of a medical device.

Consider the *Consistency* design principle in the ANSI/AAMI 62366 standard. This principle recommends that a UI design be consistent in its layout, screen structure, navigation, terminology, and control elements. Following the above process, our method interprets it as the following casual factors categories:

- **Inconsistency of feedback.** Feedback for control actions or events that are conceptually similar is not provided using the same modalities (e.g., visual, auditory, haptic). *Rationale: Inconsistent feedback leads to confusion.*
- **Inconsistency of controls:** The same UI controls produce different effects in conceptually similar situations, or, conversely, UI controls that are conceptually similar require different interaction styles. *Rationale: Consistent controls facilitate the formation of accurate and complete mental models of how to interact with the system.*
- **Inconsistency with clinical workflows:** Workflows supported by the UI software are not consistent with best or actual clinical practices. *Rationale: The UI software design should support and enhance existing clinical workflows rather than disrupting them.*
- **Inconsistency with user manuals:** Workflows described in the user manual are not consistent with the behavior of the device. *Rationale: The software development process should produce user manuals that are correct with respect to the UI software functions.*

3 Initial evaluation

We have carried out an initial evaluation of the applicability and potential benefit of our method on the Gantry-2 system, an experimental radiation therapy device for advanced cancer treatment. The Gantry-2 system consists of automated controllers for managing the delivery of radiation to the patient, and

[3] To be more specific, unsafe control actions by human operators.

beamline sensors and cameras for monitoring the patient status and the overall treatment process. Human operators are responsible for setting up the system, starting the treatment, and monitoring the patient and the device state, which are carried out using controls and displays on the system's consoles. Full details of STPA control models for the system can be found in [1].

A team of researchers have applied the standard STPA to analyze the UI design of the Gantry-2 system, based on its preliminary design documents [1]. We applied the new casual factors categories to the same system and compare our results with [1]. To ensure a fair comparison, our study was based on the same set of design documents, and the same control model and system boundaries, as those considered in the original study.

Our study showed that our method enabled us to identify not only all design issues reported in [1] but also new critical UI software design issues. An example design issue detected by our method, but not by the standard STPA method, is as follows:

Design issue: *The UI displays 'patient not ready' alerts on the main console but not on the remote console.*

Scenario: *The operator erroneously starts the treatment because inconsistent alerts are shown on the two consoles, resulting in a situation where the operator has an incorrect understanding of the patient readiness status.*

This issue can be easily identified by applying the aforementioned *Inconsistency of Feedback* category to the alerts displayed by the Gantry-2 consoles. Other example design issues identified using our method can be found in [5].

4 Conclusion

We have presented a method for enhancing the STPA causal factors categories to support systematic identification of UI software design in medical devices that likely induce use errors. Initial evaluation demonstrates that our method enables the identification of subtle UI software design issues that are difficult to detect with the standard STPA categories. Future research includes investigating ways to mechanize the instantiation of the casual factor categories to a specific design principle.

Acknowledgments. Sandy Weininger (FDA), Scott Thiel (Navigant Consulting, Inc.), Michelle Jump (Stryker), Stefania Gnesi (ISTI/CNR) and the CHI+MED team (`www.chi-med.ac.uk`) provided useful feedback and inputs. Paolo Masci's work is supported by the North Portugal Regional Operational Programme (NORTE 2020) under the PORTUGAL 2020 Partnership Agreement, and by the European Regional Development Fund (ERDF) within Project "NORTE-01-0145-FEDER-000016".

References

1. Blandine, A.: System Theoretic Hazard Analysis applied to the risk review of complex systems. Ph.D. thesis, MIT (2012)
2. de Boer, R.J., de Jong, S.: Application of stamp to facilitate interventions to improve platform safety. In: Proceedings of the 3rd STAMP workshop, boston (2014)

3. Dokas, I., Feehan, J., Imran, S.: EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. Safety Science 58, 11–26 (2013), https://doi.org/10.1016/j.ssci.2013.03.013
4. Food and Drug Administration (FDA): Class 2 Device Recall ACCUCHEK Connect Diabetes Management App (2015), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=134687
5. Masci, P., Zhang, Y., Jones, P., Campos, J.C.: A hazard analysis method for systematic identification of safety requirements for user interface software in medical devices. In: International Conference on Software Engineering and Formal Methods. pp. 284–299. Springer (2017)
6. Nielsen, J.: Usability engineering. Morgan Kaufmann (1993), https://doi.org/10.1016/B978-0-08-052029-2.50001-2
7. Thornberry, C.: Extending the Human-Controller Methodology in Systems-Theoretic Process Analysis (STPA). Ph.D. thesis, MIT (2014)