SafeSecRETS: A Project Planning Tool for Critical IoT Systems

Ernesto Fonseca Veiga[0000−0001−8255−2850], Karlla Loane Santos Lima[0009−0002−9500−8605], Taciana Novo Kudo[0000−0002−7238−0562], and Renato de Freitas Bulcão-Neto[0000−0001−8604−0019]

Instituto de Informática, Universidade Federal de Goiás, Goiânia, Goiás, Brazil
{ernestoveiga, karllaloane}@discente.ufg.br, {taciana, rbulcao}@ufg.br

Abstract. Assuring safety and security from the earliest stages of development in critical IoT systems requires a clear understanding of the system's objectives, boundaries, and operational context. This paper presents *SafeSecRETS*, a software tool for agile project planning of critical IoT systems. Through a canvas-based approach, *SafeSecRETS* supports requirements engineers and stakeholders in project scope definition and system requirements elicitation. The tool features a collaborative pipeline with interconnected building blocks, fostering engagement among information, people, and decision-making. Moreover, it assists in identifying key elements of the critical IoT system, such as components, safety and security aspects, and potential risks, by preparing the requirements analysis and specification through methods based on STPA (Systems Theoretic Process Analysis). Built on a layered event-driven architecture, *SafeSecRETS* leverages modern, scalable technologies to provide a high-quality web application. We also demonstrate how the tool supports the planning of an automated insulin delivery system.

Keywords: Safety, Security, IoT, Planning, Canvas.

1 Introduction

Effective planning is crucial to a project's success and closely tied to the Requirements Engineering (RE) process [9]. Both project planning and RE involve defining and analyzing scope, making their integration at the project's outset highly beneficial. However, many organizations face challenges in adopting effective planning practices [12], particularly when managing complex projects and coordinating diverse stakeholders, as in critical IoT systems [14].

Safety and security are essential requirements extensively studied in critical IoT systems [8]. Safety refers to a system's ability to operate without failures that could harm people or the environment, addressing accidental risks with no malicious intent; in contrast, security focuses on protecting the system from both accidental and deliberate intrusions, mitigating risks arising from malicious intent [8]. Addressing safety and security requirements early in the development life cycle of critical systems is crucial for a project's quality [14].

Proceedings of the 28th Workshop on Requirements Engineering (WER2025),
August 20-22, 2025, Rio de Janeiro-RJ, Brazil.
https://doi.org/10.29327/1588952.28-22

In this context, Leveson and Thomas [7] developed *System-Theoretic Process Analysis* (STPA), a proactive hazard analysis method that identifies accident causes, enabling early hazard mitigation. However, STPA primarily targets safety. Recognizing similar challenges in security, and the need for alignment between these requirements, several studies have proposed extensions or adaptations of STPA to meet safety and security [4–6, 16, 11].

In prior work [13, 14], we introduced *SafeSecIoT Canvas*, a strategic and visual artifact for planning critical IoT projects that covers the gap between project planning to STPA-based safety and security analysis. This canvas structures *fundamental questions* into interconnected *building blocks*, facilitating scope definition and project information capture in a single board. Visual tools are increasingly adopted to enhance communication and collaboration, making planning more practical and accessible than traditional methods. The canvas approach fosters stakeholder engagement by improving the clarity and organization of ideas [3, 10]. However, despite its potential benefits to support STPA-based methods, no existing approach or software tool currently supports these artifacts.

To address this gap, this work presents the *SafeSecRETS* software tool, a *SafeSecIoT Canvas*-based solution for agile project planning and supporting STPA-based analysis. The tool aims to facilitate project scope definition and the systematic collection of essential information for conducting STPA-based safety and security requirements analysis and specification. As a proof of concept, the *SafeSecRETS* was applied to the project planning and preparing STPA-based analysis of a critical IoT system for automated insulin delivery (AID).

This paper is organised as follows: Section 2 presents theoretical background; Section 3 analyses related work; Section 4 describes the *SafeSecRETS* tool; Section 5 presents a tool usage demo; and Section 6 brings final remarks.

2 Background

In prior research, we proposed *MM4Canvas* [13], a metamodel providing a structured method for developing canvas models. It defines the fundamental questions to structure project planning. The metamodel enables the creation of building blocks that address these questions in alignment with the canvas model's objective. These blocks can be: i) general-purpose, covering broad planning concepts (e.g., project or business-oriented); or ii) domain-specific, tailored for specialized requirements (e.g., IoT, safety, security).

The *SafeSecIoT Canvas* model is an instance of the *MM4Canvas* metamodel for agile project planning in critical IoT systems. To achieve this goal, first, we instantiate a conceptual model based on the components and relationships of the *Project Model Canvas* (PMC) [3]. Next, we reuse PMC general-purpose components, addressing essential project planning concepts. We extend this model with domain-specific components to handle concepts and specific concerns of critical IoT systems, such as safety and security, and prepare STPA-based analysis [14].

The IoT domain-specific building blocks for *SafeSecIoT Canvas* [1] are: i) components: hardware/software elements, including sensors, actuators, and al-

gorithms for identification, control, and orchestration; ii) connectivity: the means enabling components communication; iii) actions: relevant system interactions; and iv) data: information generated by components. Regarding safety and security [7], the blocks include: i) assets: valuable elements requiring protection (people, resources, environment, or services); ii) losses: unacceptable damages from accidents or attacks; and iii) risks: potential causes of losses, whether intentional or accidental. These blocks will serve as inputs for the STPA-based analysis, according to the approach presented in Veiga et. al [14].

3 Related Work

With the rise of critical systems requiring safety-security alignment, research has focused on integrating co-analysis through STPA extensions [4–6, 16, 11]. Friedberg et al.[4] propose linking an abstract control structure to the physical system design to incorporate traditional security analysis. Ribeiro et al. [11] explore an STPA-based safety and security RE process for autonomous vehicle development. Zhou et al. [16] and Gomola and Utne [6] focus on eliminating or mitigating hazards based on identified loss scenarios.

Glomsrud and Xie [5] identified a gap in the initial steps of STPA (which also extends to its extensions), highlighting challenges in transitioning from Step1 (defining the purpose) to Step2 (modeling the control structure), especially with limited prior knowledge of the system. To address this, Veiga et al. [14] incorporate a project planning artifact into an STPA-based safety and security analysis method [15], enhancing analysis purpose definition, control structure modeling, and requirement specification. However, to our knowledge, no prior work offers tools to enhance the initial stages of safety and security STPA-based analysis.

Building on artifacts proposed in our previous works and aiming to support other STPA-extended approaches, this paper introduces a collaborative tool for project planning at the outset of STPA analysis. The tool facilitates scope definition and the identification of essential project information. Using a canvas-oriented approach, it structures key data into building blocks that serve as inputs for the subsequent STPA-based analysis.

4 *SafeSecRETS* Overview

SafeSecRETS (acronym for **Saf**ety and **Sec**urity **R**equirements **E**ngineering for Critical Io**T** **S**ystems) is a collaborative canvas-based web software tool for project planning of critical IoT systems. Developed with Bubble and Supabase[1], it offers a structured pipeline for project planning and requirements elicitation. The tool features a set of interconnected building blocks, presented gradually in groups of correlated blocks (aimed at answering a fundamental question of the project), supporting multi-user collaboration and real-time project updates.

[1] Bubble: https://bubble.io/ and Supabase: https://supabase.com/

4.1 Requirements, Architecture and Development

Funcional and non-functional requirements The main functional requirements of *SafeSecRETS* tool include but are not limited to: user account management; software project management; multiple users in a project for collaborative work; canvas-based building blocks for project planning; interactive pages for information gathering; and the display of the *SafeSecIoT Canvas* to provide a project overview. Non-functional requirements include i) usability: intuitive and interactive interface aligned with UI/UX principles for a seamless user experience; ii) scalability: an event-driven architecture must support increasing concurrent users without efficiency loss; iii) security: access control and authentication must restrict event reception and data modifications to authorized clients; iv) performance: asynchronous WebSocket communication must enable real-time updates in multi-user projects, minimizing latency and database load; v) persistence and reliability: the database must ensure ACID compliance for secure, consistent operations. Furthermore, the project planning process follows the guidelines of the international standard ISO/IEC/IEEE 15288 [14].

System Architecture Fig. 1 presents the system architecture of the *SafeSecRETS*, that combines the principles of modularity and separation of responsibilities of layered architecture with the reactivity and decoupling of event-driven architecture (EDA). The architecture layers and its elements are explained next.

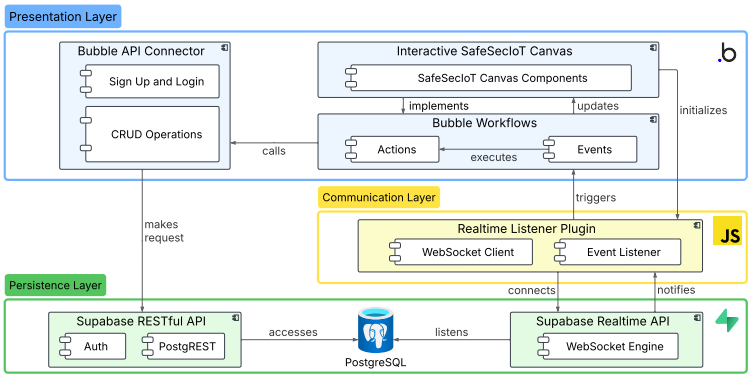

Fig. 1. *SafeSecRETS* architecture.

– *Presentation Layer (Bubble)*: It manages the tool's graphical interface, enabling users to interact with *SafeSecIoT Canvas* building blocks for project planning. Built with Bubble, a no-code platform for dynamic and interactive interfaces, it defines the workflow logic for processing user events and communicating with the backend. Its key components are i) Interactive *SafeSecIoT Canvas*: visually represents project building blocks; ii) Bubble Workflows: handle navigation, updates, and backend interactions; and iii) Bubble

API Connector: integrates external APIs like Supabase for authentication and CRUD operations. User interactions with *SafeSecRETS* trigger Bubble Workflows, executing actions such as API calls to Supabase.

- *Communication Layer (Realtime Plugin)*: It acts as a bridge between the backend and frontend, enabling Bubble to receive real-time database updates. Implemented as a Bubble plugin, it connects to Supabase Realtime via WebSockets, eliminating constant database queries and enhancing performance. Its core components are i) WebSocket Client: maintains a persistent connection with Supabase Realtime; and ii) Event Listener: subscribes to specific events (insert, update, delete). When a change occurs in monitored tables, the plugin triggers an event in Bubble, dynamically updating the UI.
- *Persistence Layer (Supabase)*: It handles project data storage and real-time communication, using Supabase, which integrates a PostgreSQL database with authentication services and REST APIs. Its key components are i) PostgreSQL: stores projects, users, and permissions; ii) Supabase Realtime: monitors database changes and transmits events via WebSockets; and iii) RESTful API: enables authentication and authorization via Supabase Auth, ensuring secure data access and modification. The Bubble application interacts with the database through Supabase's RESTful API, while Supabase Realtime notifies the plugin via WebSockets upon data updates.

Development and Technologies *SafeSecRETS* was developed using: (i) Bubble, a no-code platform for creating web applications with a visual editor for UI design, logic, and database management, API integration and JavaScript support; and (ii) Supabase, a backend-as-a-service platform offering a PostgreSQL database and integrated APIs for authentication, storage, and real-time features.

4.2 Canvas Approach for Project Planning and STPA Analysis

SafeSecRETS implements the *SafeSecIoT Canvas* [13], which comprises 20 building blocks for project planning, as illustrated in Fig. 2 (i). These blocks are grouped into five groups based on fundamental questions, providing a logical structure to scope definition. Blocks are interconnected and may relate, helping identify inconsistencies and understand the impact of changes across the project.

The first group, Project Rationale, addresses *why* the project is being undertaken. The second, Project Scope, defines *what* must be delivered and is subdivided into three parts: product and system requirements, IoT-specific elements, and safety & security considerations. The third group, Stakeholders and Team, identifies *who* is involved and their roles. The fourth, Planning Parameters, defines *how* the project will be executed, including delivery phases and constraints. The fifth, Management Parameters, addresses *when* deliverables are due, *how much* the project will cost, and potential risks and uncertainties. Each block includes guidelines and shows its relationships with other blocks, with direct navigation links to improve user experience.

Currently, *SafeSecRETS* supports collaborative project planning via the canvas. The integration with STPA-based analysis is under development.

5 Tool Demonstration

To demonstrate the capabilities of *SafeSecRETS*, we planned a critical IoT system for automatic insulin delivery (AID). These systems connect a continuous glucose monitor (CGM) to an insulin pump (IP) [2], automatically adjusting insulin doses to regulate blood glucose levels in patients with type 1 diabetes. Due to their modular hardware and software design, AID systems pose significant safety and security challenges. Precision and reliability are essential for patient health, while system failures or cyber-attacks can jeopardize data integrity or cause serious harm.

Fig. 2 illustrates how *SafeSecRETS* supports the planning of such systems. Upon logging in, the user is directed to the Home screen, where they can create or access projects. Selecting a project opens the complete canvas view (i), which organizes building blocks by their logical relationships and suggests an order for filling them out. Within the Project Scope section, specific groups of blocks (ii and iii) guide the description of the system's IoT components and its safety and security aspects - elements that are particularly relevant to critical systems like AID. When users open a building block for editing (iv), they receive guidelines, information about related blocks, and navigation links to enhance their understanding and ensure structured input.

These features demonstrate how the tool facilitates an AID system's structured and comprehensive planning process. By explicitly guiding users through identifying project rationale, system requirements, IoT components, and safety and security-critical elements, the tool helps ensure that essential concerns are addressed from the early stages of system design. In critical IoT systems, such as AID systems, where failures or vulnerabilities can directly affect patient health, the canvas not only supports a clearer understanding of system architecture and its associated risks but also promotes more informed decision-making, supporting the subsequent analysis and specification of safety and security requirements tailored to the context of critical IoT applications.

6 Final Remarks

This article introduces and highlights the importance of the *SafeSecRETS* as a practical solution to address gaps in the project planning of critical IoT systems and support the STPA-based analysis method in specifying safety and security requirements. Its relevance lies in its potential to facilitate and enhance the RE process, aiming to ensure a positive user experience and promote collaborative work between stakeholders.

Future work includes developing a new module to support the STPA-based safety and security RE process, from defining the analysis purpose to specifying requirements. We also plan to execute experiments with STPA experts in the critical IoT systems domain to assess the tool thoroughly.

The tool is available at: https://safesecretstool.bubbleapps.io/version-test/.
Tool's Video: https://youtu.be/CMWIR0nJXls

Fig. 2. *SafeSecRETS* user interface: (i) the complete *SafeSecIoT Canvas* view for a project; (ii)–(iii) screens of the IoT and Safety & Security groups within the Project Scope; and (iv) the Losses building block with filling guidelines and related connections.

References

1. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey. Computer Networks **54**(15), 2787–2805 (2010). https://doi.org/https://doi.org/10.1016/j.comnet.2010.05.010
2. Deshpande, S., et al.: Design and Clinical Evaluation of the Interoperable Artificial Pancreas System (iAPS) Smartphone App. Diabetes Technology & Therapeutics **21**(1), 35–43 (2019). https://doi.org/10.1089/dia.2018.0278
3. Finocchio-Júnior, J.: Project Model Canvas. Elsevier Brasil (2013)
4. Friedberg, I., et al.: STPA-SafeSec: Safety and security analysis for cyber-physical systems. Journal of Information Security and Applications **34**, 183–196 (2017). https://doi.org/https://doi.org/10.1016/j.jisa.2016.05.008
5. Glomsrud, J.A., Xie, J.: A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships. In: 29th European Safety and Reliability conference (2019). https://doi.org/10.3850/978-981-11-2724-3_0105-cd
6. Gomola, A., Bouwer Utne, I.: A novel STPA approach to software safety and security in autonomous maritime systems. Heliyon **10**(10) (May 2024). https://doi.org/10.1016/j.heliyon.2024.e31483
7. Leveson, N.G., Thomas, J.: STPA Handbook. MIT (2018)
8. Lyu, X., Ding, Y., Yang, S.H.: Safety and security risk assessment in cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications **4**(3), 221–232 (2019). https://doi.org/https://doi.org/10.1049/iet-cps.2018.5068
9. Nawrocki, J., et al.: Agile Requirements Engineering: A Research Perspective. In: SOFSEM: Theory and Practice of Computer Science. pp. 40–51. Springer International Publishing (2014). https://doi.org/10.1007/978-3-319-04298-5_5
10. Osterwalder, A., Pigneur, Y.: Business Model Generation: a handbook for visionaries, game changers, and challengers, vol. 1. John Wiley & Sons (2010)
11. Ribeiro, Q., Castro, J.: Safety & Security Alignment in Requirements Engineering Process for Autonomous Vehicles. In: Anais do WER 2022 - Workshop em Engenharia de Requisitos (2022). https://doi.org/10.29327/1298262.25-25
12. Rosacker, K.M., Rosacker, R.E.: Information technology project management within public sector organizations. Journal of Enterprise Information Management **23**(5), 587–594 (2010)
13. Veiga, E.F., Kudo, T.N., Bulcão-Neto, R.F.: A Canvas Metamodel to Bridging Agile Project Planning and Requirements Engineering. In: Proceedings of the WER24 (2024). https://doi.org/10.29327/1407529.27-18
14. Veiga, E.F., Kudo, T.N., Bulcão Neto, R.F.: Linking Agile Planning and Safety and Security Analysis in Critical IoT Systems: An Approach based on ISO/IEC/IEEE 15288. In: Proceedings of the XXIII Brazilian Symposium on Software Quality. p. 81–91. SBQS '24, ACM (2024). https://doi.org/10.1145/3701625.3701648
15. Veiga, E.F., Bulcão Neto, R.F.: Toward a Method for Safety and Security Requirements Alignment in Critical IoT Systems. In: Proceedings of the XXXVII Brazilian Symposium on Software Engineering. p. 452–457. SBES '23, ACM (2023). https://doi.org/10.1145/3613372.3613373
16. Zhou, X.Y., Liu, Z.J., Wang, F.W., Wu, Z.L.: A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Engineering **222** (2021). https://doi.org/https://doi.org/10.1016/j.oceaneng.2021.108569