Integrating Goal Oriented Requirements Modeling and Safety Analysis with RESafety

Moniky Ribeiro [1], Jaelson Castro [1], Ricardo Argenton [2], Maria Lencastre [3], Abimael Santos [1], Oscar Pastor [4]

[1] Universidade Federal de Pernambuco, Av. Prof. Moraes Rego, 1235 - Cidade Universitária, Recife - PE, Brazil
[2] Universidade Federal do Vale do São Francisco, Av. José de Sá Maniçoba - Centro, Petrolina – PE, Brazil
[3] Universidade de Pernambuco, Agamenon Magalhães, S/N - Santo Amaro, Recife – PE, Brazil
[4] Universidad Politécnica de Valencia, Camí de Vera, s/n, 46022 València- Valencia, Spain

Abstract

Safety properties of Critical Systems must be identified and modeled as early as possible. Yet, the Requirements Engineering and Safety Engineering communities often do not make efforts to integrate their best practices. Therefore, it is worth considering the alignment of new goal-oriented safety requirements modeling languages with modern safety analysis approaches. The goal of this research is to propose a new approach, called RESafety, that aligns early safety requirements modeled in iStar4Safety language with safety elements identified through STPA (System-Theoretic Process Analysis), a system approach to hazard analysis.

Keywords

Goal Oriented Requirements Modeling, Safety-Critical Systems, iStar4Safety

1. Background and Motivation

Safety Critical Systems (SCSs) are considered systems that, if they fail or behave unexpectedly, can lead to accidents that may damage people, environment property, as well as may cause loss of life or finance [1]. Safety must be considered since the beginning of the SCS development process until the end of its useful life [2]. Safety is an emergent property, therefore the safety of a system is more than safety of its components. It should consider the safety of its interfaces and the safety of complex interactions between system´s components and people[3]. Unfortunately, classic safety analysis approaches like HAZOP, FTA, and FMEA do not consider safety an emergent property. Moreover, these approaches were formulated when computing systems did not yet exist [1]. In contrast, the STPA technique regards safety as an emergent property [3].

Requirements Engineering is one of the most crucial phases for the development of quality systems, as unclear or missing requirements can negatively impact the quality of the Technical Social System [4]. GORE (Goal-Oriented Requirements Engineering) is commonly used in the early requirements phase [5]. Goal-oriented languages such as iStar, KAOS, and GRL can be used to organize and justify software requirements, especially in the early stages. iStar has gained widespread interest in the requirements community and has over a hundred extensions [6]. iStar4Safety, adds concepts related to Preliminary Safety Analysis [7].

The goal of our research is to promote safety analysis during the early stages of development to identify and model safety requirements as early as possible. In this paper we report on the development of the RESafety approach. This ongoing project intends to align the iStar4Safety language, which is used during the early phase requirements, with the STPA safety analysis technique [3].

iStar'23: The 16th International i* Workshop, September 3rd–4th, 2023, Hannover, Germany

smsr@cin.ufpe.br (S. Ribeiro); jbc@cin.ufpe.br (J. Castro); ricardo.aramos@univasf.edu.br (R. Argenton) , mlpm@ecomp.poli.br (M. Lencastre), ajfs@cin.ufpe.br (A. Santos), opastor@dsic.upv.es (O. Pastor)

0000-0002-4834-6647 (S. Ribeiro); 0000-0002-4635-7297 (J. Castro); 0000-0002-9688-719x (R. Argenton), 0000-0002-8032-8801 (M. Lencastre), 0009-0003-7555-6927 (A. Santos), 0000-0002-1320-8471 (O. Pastor)

2. Goal modeling for Safety Critical Systems

It is crucial to pay close attention to the requirements phase when dealing with Safety-Critical Systems. Ensuring that the specifications are correct and accurate is essential, as many mistakes in requirements can lead to disasters.

GORE languages aim to improve the understanding and communication of requirements among stakeholders and facilitate the development of systems that meet their goals and expectations. By emphasizing goals, it allows for a broader perspective of the system and stakeholder needs, reducing the focus on any specific system view [5].

GORE languages can be particularly useful in safety-critical systems where clear and unambiguous requirements are essential for ensuring the system's reliability and safety [11].

Safety standards such as EN50126 (CEN, 2000) [8] or EN50128 (CEN, 2001) [9] advocate the need to support design and development activities with semi-formal notations and model-based development approaches [10]. Models provide a way of understanding the phenomena, enabling their representation in a more understandable way through the abstraction of the real world.

3. RESafety Approach

Our approach, named RESafety, enables the early modeling and analysis of safety requirements. It consists of a set of steps.

STEP 1 – Identify Actors:

When designing a SCS, it is crucial to identify the relevant stakeholders, which includes people, or, internal and external systems. Strategic stakeholders will be mapped to actors in iStar4Safety.

STEP 2 – Define iStar4Safety Models:

Once the actors have been identified, create the dependency model. The following y guidelines may be useful:

- **Guideline 1:** Create a standard model without safety elements (non-safety related part);
- **Guideline 2:** Consider the safety goal of interest;
- **Guideline: 3** Insert all hazards related to the safety goal of interest;
- **Guideline 4:** Identify all causes for each identified hazard. The causes are the hazard-child of the hazard;
- **Guideline 5:** Define the mitigation strategy for each leaf hazard – i.e., the safety resources and safety tasks that should be used to mitigate each leaf hazard;
- **Guideline 6:** Associate the mitigation strategy with an actor which will be responsible for its achievement through dependency links.

Guideline 2 through 6 must be repeated in successive iterations until all safety requirements are appropriately dealt with.

STEP 3 – Consequences of a safety goal not being satisfied:

We are currently considering the use BPMN for the description of the consequences of a safety goal not being satisfied [11].

STEP 4 – Define STPA Analysis:

In order to carry out the STPA safety analysis the following actions must be performed [3]:

– Action 1: Definition of the purpose of the analysis;

– Action 2: Control structure modeling;
– Action 3: Identification of UCAs - Unsafe Control Actions;
– Action 3: Identification of loss scenarios.

Note that iStar4Safety models created in **STEP 2** and the BPMN process models of **SEP 3** are input to **STEP 4** (STPA analysis).

STEP 5 – Update initial modeling:
After the STPA analysis (**STEP 4**) the iStar4Safety and BPMN models.

3.1. RESafety Illustration

In this section, we provide a short illustration of the use of our approach in the context of an insulin infusion pump. It was used based on previous iStar4Safety models [7] and STPA analysis [13].

STEP 1 – Identify System Actors:
The actors related to the *Insulin Infusion Pump System* initially considered in [7] include patient, and pump, among others. Given the limited space and the importance of the patient actor, we will focus on it to illustrate our proposal.

STEP 2 – Define iStar4Safety's Models:
We use iStar4Safety to model the patient actor (see Fig. 1). Consider that this is an initial model meeting the goals of the early requirements analysis. Therefore, the view in this model is high-level one. Setting up the pump to deliver the correct basal infusion is a quite critical safety goal (see Figure 1).

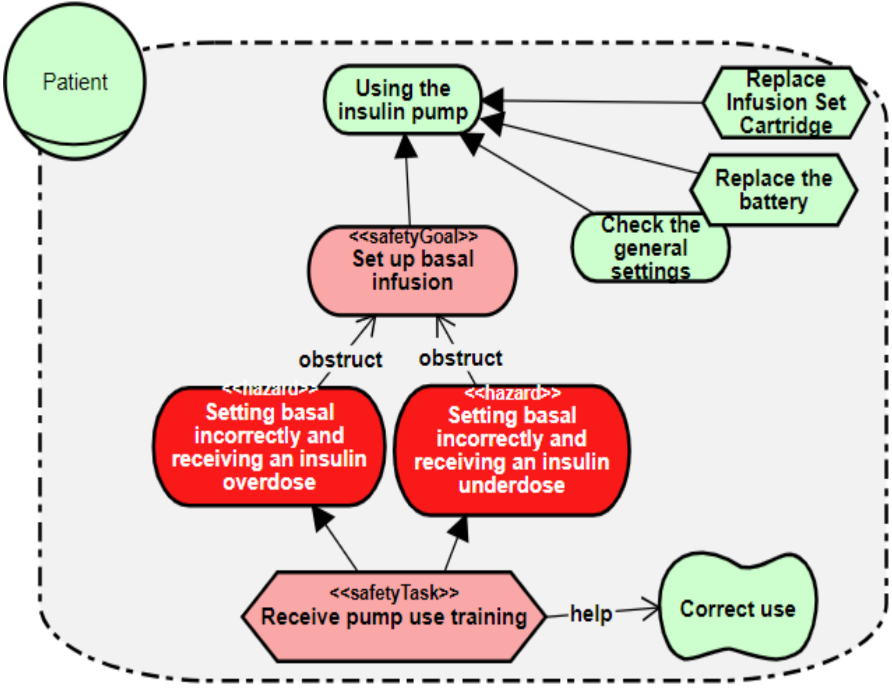
Patient
Using the insulin pump
Replace Infusion Set Cartridge
Replace the battery
Check the general settings
<<safetyGoal>> Set up basal infusion
obstruct
obstruct
<<hazard>> Setting basal incorrectly and receiving an insulin overdose
<<hazard>> Setting basal incorrectly and receiving an insulin underdose
<<safetyTask>> Receive pump use training
help
Correct use

Figure 1 - Excerpt of the SR model of Patient Actor. Adapted from [15].

After some more careful analysis, we may consider the need to refine the Safety Goal "Set up basal Infusion" to consider two hazardous situations related to wrong setting of the pump, which may lead to an overdose or underdose of insulin (see Fig 1).

STEP 3 – Expand safety goals using process modeling:

It may be worth describing what happens if a safety goal (e.g. "Set up basal infusion") is not satisfied. A BPMN diagram with more details of other adverse consequences could be created, but the scenario treated in this work was reduced due to space limitation.

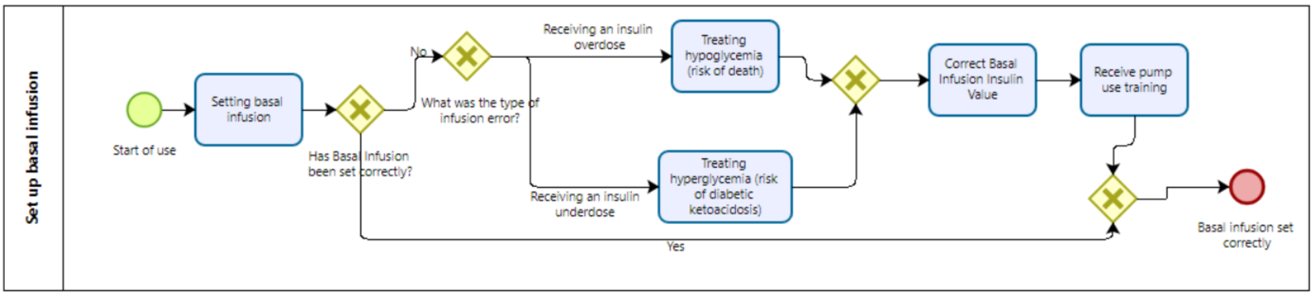
Set up basal infusion
Start of use
Setting basal infusion
Has Basal Infusion been set correctly?
No
What was the type of infusion error?
Receiving an insulin overdose
Treating hypoglycemia (risk of death)
Receiving an insulin underdose
Treating hyperglycemia (risk of diabetic ketoacidosis)
Correct Basal Infusion Insulin Value
Receive pump use training
Yes
Basal infusion set correctly

Figure 2 - Excerpt of the BPMN description of the safety goal not being satisfied.

STEP 4 – Define STPA Analysis:

The initial iStar4Safety model (e.g. Fig 1) and Process model (e.g. Fig 2) can be considered as input to the STPA analysis, as the one conducted in Martinazzo [14]. In his analysis, safety requirements were specified to deal with the hazards of hyperglycemia, hypoglycemia, glycemic variations, and dermatological problems.

STEP 5 – Update initial modeling:

Having performed that STPA analysis, it is necessary to update the previous iStar4Safety and BPMN models. Due to space limitation an excerpt of the revised Patient in iStar4Safety model is depicted in Fig. 3.

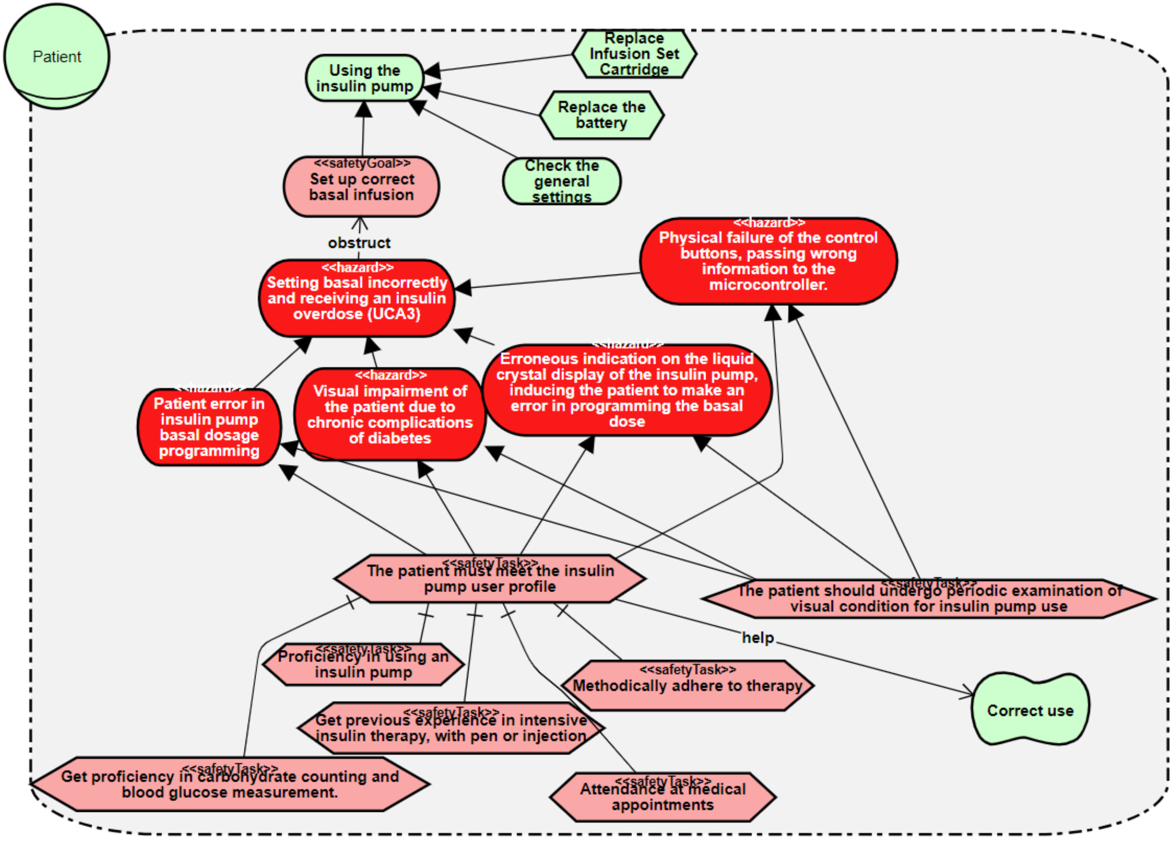
Patient
Using the insulin pump
Replace Infusion Set Cartridge
Replace the battery
Check the general settings
<<safetyGoal>> Set up correct basal infusion
obstruct
<<hazard>> Setting basal incorrectly and receiving an insulin overdose (UCA3)
<<hazard>> Physical failure of the control buttons, passing wrong information to the microcontroller.
<<hazard>> Patient error in insulin pump basal dosage programming
<<hazard>> Visual impairment of the patient due to chronic complications of diabetes
<<hazard>> Erroneous indication on the liquid crystal display of the insulin pump, inducing the patient to make an error in programming the basal dose
<<safetyTask>> The patient must meet the insulin pump user profile
<<safetyTask>> The patient should undergo periodic examination of visual condition for insulin pump use
help
Correct use
<<safetyTask>> Proficiency in using an insulin pump
<<safetyTask>> Methodically adhere to therapy
<<safetyTask>> Get previous experience in intensive insulin therapy, with pen or injection
<<safetyTask>> Get proficiency in carbohydrate counting and blood glucose measurement.
<<safetyTask>> Attendance at medical appointments

Figure 3 - Excerpt of the Revised Patient Actor.

4. Related Work

To the best of our knowledge, our approach it the only one relying on goal modeling (iStar4Safety), BMPN and STPA. Below we discuss some related work.

Sharifi et al. [12,13] present a proposal to assist in the certification of FinTech that combines the advantages of the goal orientation of the GRL language with the process modeling of the UCM language. They start using the onion model for stakeholder identification. As a next step, the GRL strategic dependency model is made. Here, the authors use various sources of information as initial artifacts, such as handbooks and interviews with stakeholders. Then, they expand the GRL model with the Use Case Maps (UCM) model, modeling as UCM the functional goals discovered in the GRL model, also allowing traceability between the models. The authors propose to carry out the STPA analysis as a next step. The artifacts created by STPA are used to update the previous models as well as to create assurance cases. The similarities between our work and [12,13] are not mere coincidence. However, there are many differences. We first deal with Safety-Critical System, creating a process that generalizes the search for safety requirements from the initial development phase. In addition, we will use the iStar4Safety GORE language[7] which already has safety constructors as first class citizens. Moreover, they rely on UCM for process modeling while we are considering the use of BPMN to describe the consequences of a safety goal not being satisfied.

Vilela et al. [15] presents the SARSSi* approach. The solution presented in their work combined STPA hazard analysis technique with the iStar goal-oriented requirements modeling technique, generating a preliminary safety analysis. An essential difference is that the former uses iStar in its standard version to model safety elements, while RESafety relies on iStar4Safety and the description of unsatisfied safety goals in BPMN.

5. Conclusions and Future Work

Our work focuses on developing the RESafety approach, which aligns iStar4Safety and STPA. iStar4Safety is a goal-oriented modeling language that can be used to model safety requirements in the early stages of safety analysis, while STPA is an analysis technique based on Systems Theory. By integrating STPA and iStar4Safety, the RESafety proposal enables a more systematic and comprehensive approach to model early safety requirements. It enhances the identification and analysis of safety-related concerns, facilitates communication among stakeholders, and supports the development of safer and more reliable systems.

We to have it evaluated by Requirements Engineering and Safety Engineering experts. To illustrate its potential, we will use RESafety to define safety requirements of at least two types of Safety-Critical Systems (Medical Domain and Transport Domain),

In future work, we intend to investigate how other qualities, such as security, reliability, etc., can interfere with the System and interact with the safety property. We will explore the need to model technical, social, and composite safety requirements differently. There is a need to clarify the navigation strategies between the steps in RESafety.

6. Acknowledgment

The authors would like to express their gratitude for the financial support provided by Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), and Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Their support has been instrumental in the successful completion of this research.

7. References

[1] N. G. Leveson, Safeware: System Safety and Computers, ACM, New York, NY, USA, 1995.

[2] N. G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Mit Press, Massachusetts, London, England, 2011.

[3] N. G. Leveson, J. P. Thomas, STPA Handbook, first ed., 2018.

[4] D. M. Berry, The safety requirements engineering dilemma, in: Proceedings of the 9th International Workshop on Software Specification and Design, IWSSD ’98, IEEE Computer Society, Washington, DC, USA, 1998.

[5] J. Mylopoulos, L. Chung, E. Yu, From object-oriented to goal-oriented requirements analysis, Communications of the ACM 42, 31–37, 1999.

[6] E. Gonçalves, M. A. de Oliveira, I. Monteiro, J. Castro, J. Araújo, Understanding what is important in iStar extension proposals: the viewpoint of researchers, Requirements Engineering, Vol 24, pp 55-84, 2019.

[7] M. Ribeiro, J. Castro, J. Pimentel, iStar for safety-critical systems, in: J. Pimentel, J. P. Carvallo, L. López (Eds.), Proceedings of the 12th International i* Workshop co-located with 38th International Conference on Conceptual Modeling (ER 2019), Salvador, Brazil, November 4th, 2019, volume 2490 of CEUR Workshop Proceedings, CEUR-WS.org, 2019.

[8] BS-EN 50126-1- Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Generic RAMS Process, 2000.

[9] CLC, EN-50128 - Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems. 2001.

[10] S. Fugivara, A. Merladet, C. Lahoz, STPA analysis of brazilian sounding rockets launching operations, Microgravity Sci. Technol. 33, 2021. IEEE, pp. 205–214, 2022.

[11] S. White, D. Miers, BPMN Modeling and Reference Guide: Understanding and Using BPMN, Business Process Management Process Modeling, Future Strategies Incorporated, 2008.

[12] S. Sharifi, P. McLaughlin, D. Amyot, J. Mylopoulos, Goal modeling for fintech certification, in: R. S. S. Guizzardi, G. Mussbacher (Eds.), Proceedings of the Thirteenth International iStar Workshop co-located with 28th IEEE International Requirements Engineering Conference (RE 2020), volume 2641 of CEUR Workshop Proceedings, CEUR-WS.org, pp. 73–78, 2020.

[13] S. Sharifi, D. Amyot, J. Mylopoulos, P. McLaughlin, R. Feodoroff, Towards improved certification of complex fintech systems - A requirements-based approach, in 2022 IEEE 30th International Requirements Engineering Conference Workshops (REW), Melbourne, Australia,

[14] A. Martinazzo, Gerenciamento de risco de uma bomba de infusão de insulina de baixo custo (in English: Risk management of a low-cost insulin infusion pump), Master’s thesis, Universidade Federal de São Paulo, 2022.

[15] J. Vilela, C. Silva, J. Castro, L. E. G. Martins, T. Gorschek, Sarssi*: a safety requirements specification method based on stamp/stpa and i* language, in: Anais do I Brazilian Workshop on Large-scale Critical Systems, SBC, Porto Alegre, RS, Brasil, 2019, pp. 17–24. URL: https://sol.sbc.org.br/index.php/bware/article/view/7504. doi:10.5753/bware.2019.7504.