RESafety

Requirements Engineering for Safety

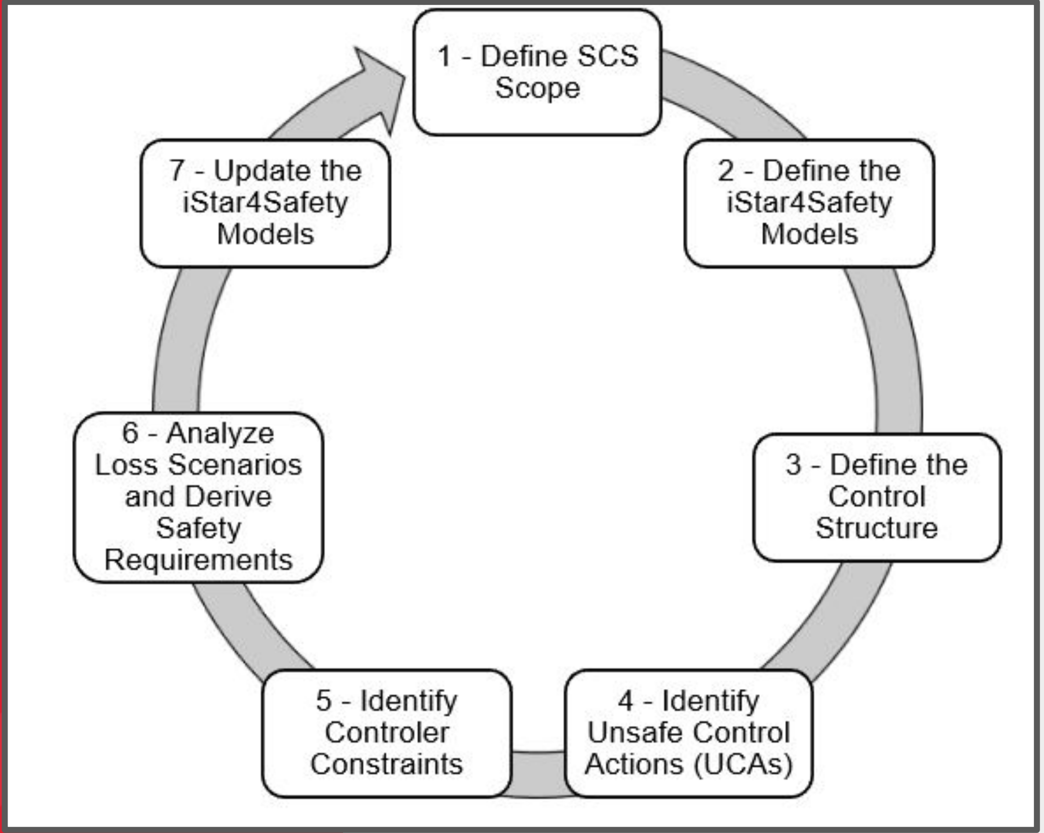
PhD Student: Moniky Ribeiro

Advisor: Prof. Jaelson Castro

Co-advisor: Prof. Ricardo Argenton

RESafety

The 7-Step Process



1 - Define SCS Scope

2 - Define the iStar4Safety Models

3 - Define the Control Structure

4 - Identify Unsafe Control Actions (UCAs)

5 - Identify Controler Constraints

6 - Analyze Loss Scenarios and Derive Safety Requirements

7 - Update the iStar4Safety Models

RESafety

Insulin Infusion Pump (IIP) Example

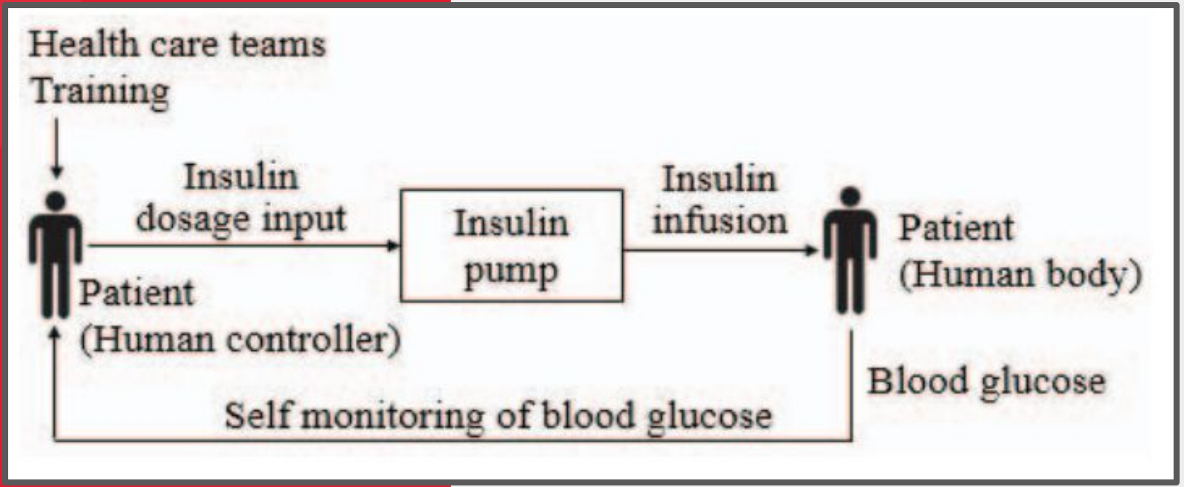
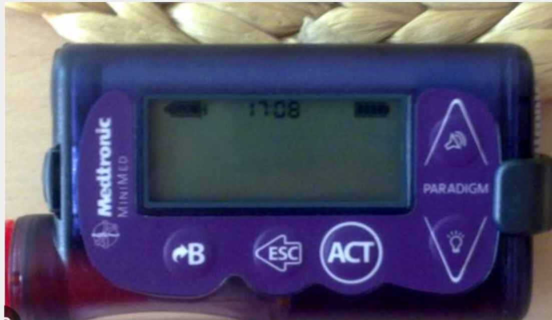


Figure 1 – Overview of the Insulin Infusion Pump System [1]



Insulin Infusion Pump (IIP)

Types of Insulin Delivery

- Basal: A constant, low-level infusion throughout the day and night. Example: Up to five programmable basal profiles over 24h.

- Bolus: A larger dose triggered by meals or to correct high blood sugar. Delivered manually or based on user programming.

Insulin Infusion Pump (IIP)

Components of a Typical Pump

- User interface: LCD screen and audio alarms.
- Hardware parts: Microprocessor, battery, infusion mechanism, insulin reservoir, and catheter.

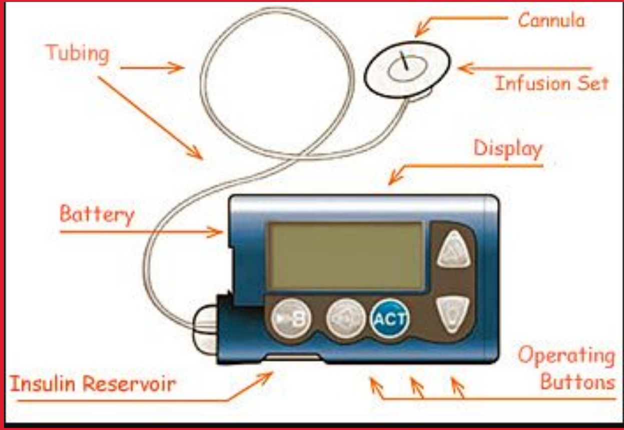


Figure 2 – Retrieved from [2]

Insulin Infusion Pump (IIP)

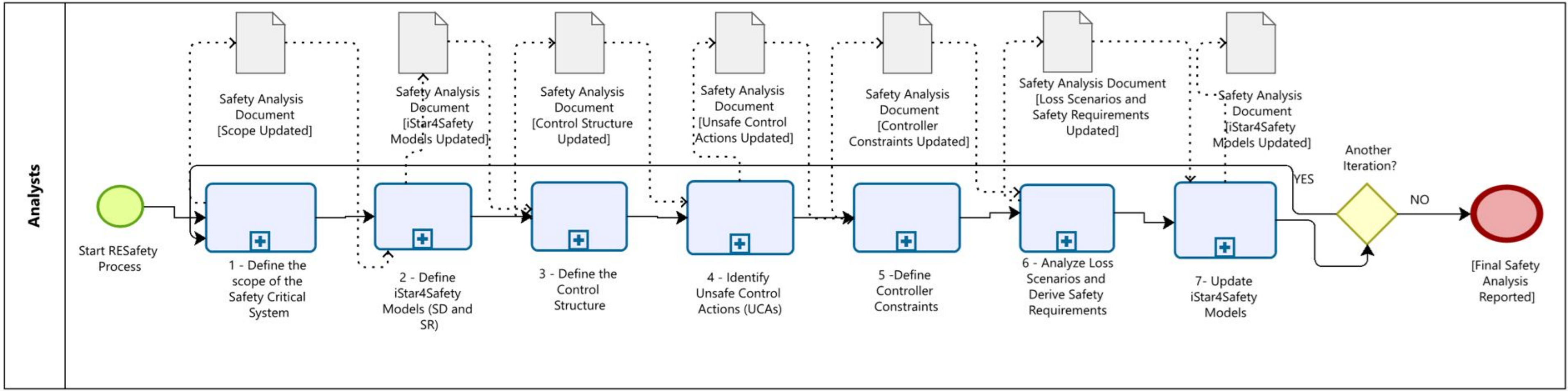
Safety implications

- Main accidents:
  - Overdose → Hypoglycemia (low blood sugar)
  - Underdose → Hyperglycemia (high blood sugar)

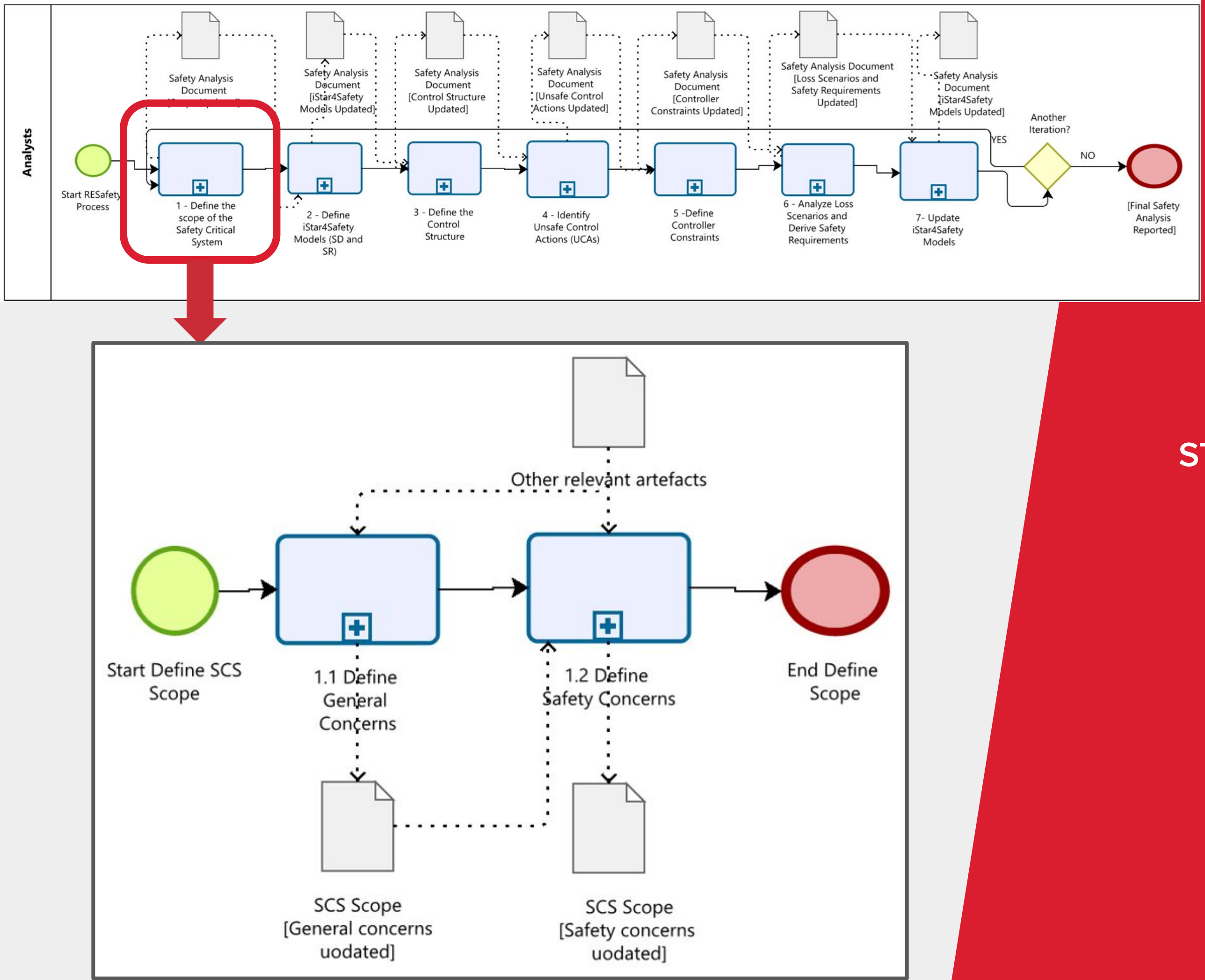
- Other accidents: skin infections, battery failure, or device malfunction, etc.

RESafety

BPMN Diagram of the Process


Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document [iStar4Safety Models Updated]
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]

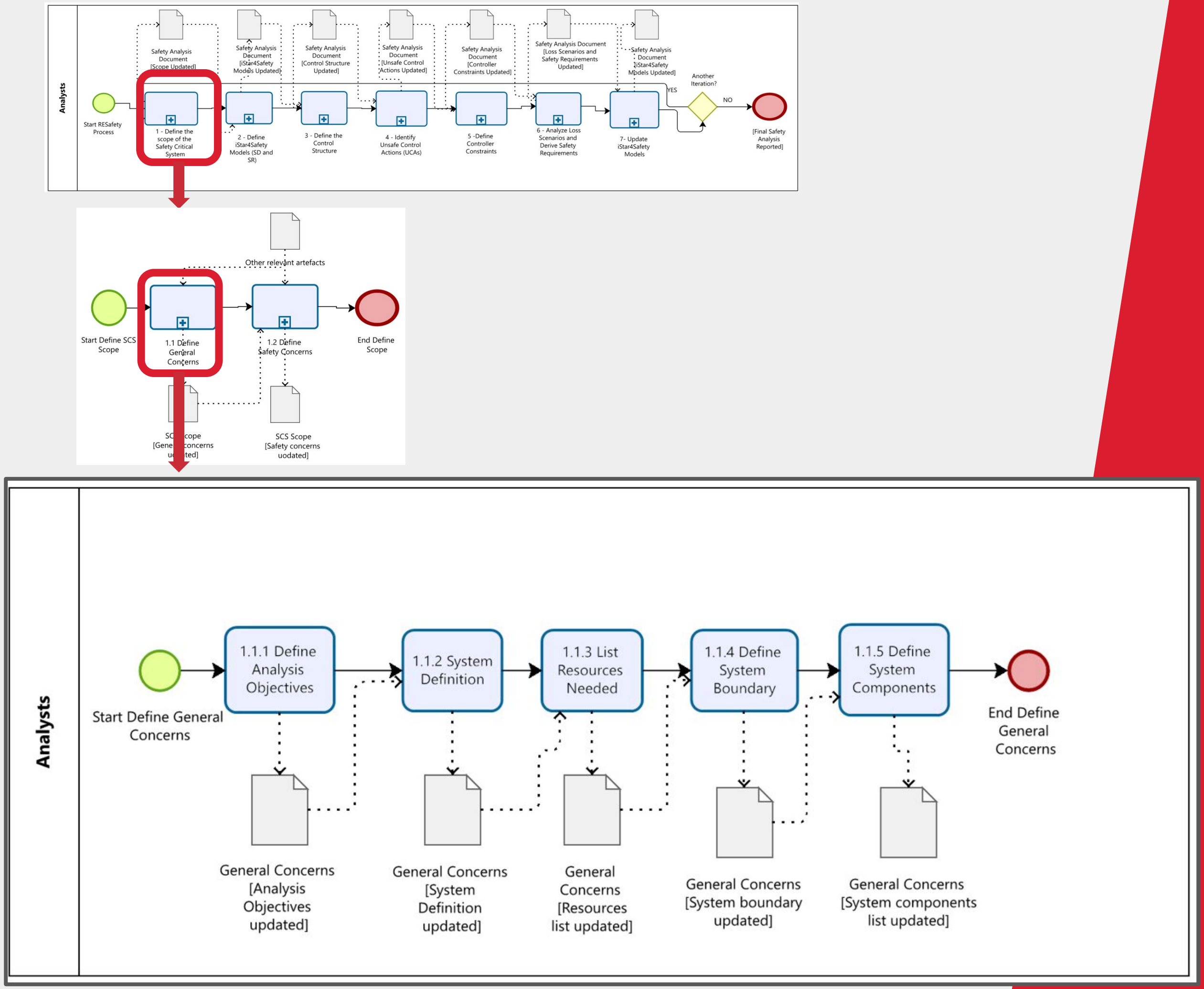
Link to the IIP Example Analysis:
https://docs.google.com/document/d/1ubwn6wNi_9WhdnSAAQxyeq6hOL1R7Ldgu0FSG1769yc/edit?tab=t.0


Analysts
Safety Analysis Document
Safety Analysis Document [iStar4Safety Models Updated]
Safety Analysis Document [Control Structure Updated]
Safety Analysis Document [Unsafe Control Actions Updated]
Safety Analysis Document [Controller Constraints Updated]
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
Safety Analysis Document [iStar4Safety Models Updated]
Another Iteration?
YES
NO
Start RESafety Process
1 - Define the scope of the Safety Critical System
2 - Define iStar4Safety Models (SD and SR)
3 - Define the Control Structure
4 - Identify Unsafe Control Actions (UCAs)
5 -Define Controller Constraints
6 - Analyze Loss Scenarios and Derive Safety Requirements
7- Update iStar4Safety Models
[Final Safety Analysis Reported]
Other relevant artefacts
Start Define SCS Scope
1.1 Define General Concerns
1.2 Define Safety Concerns
End Define Scope
SCS Scope [General concerns uodated]
SCS Scope [Safety concerns uodated]

RESafety

STEP 1 - Define the scope of the Safety-Critical System

RESafety


Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document [iStar4Safety Models Updated]
7- Update iStar4Safety Models
YES
Another Iteration?
NO
[Final Safety Analysis Reported]
Other relevant artefacts
Start Define SCS Scope
1.1 Define General Concerns
1.2 Define Safety Concerns
End Define Scope
SC cope [Gene concerns u ted]
SCS Scope [Safety concerns uodated]
Analysts
Start Define General Concerns
1.1.1 Define Analysis Objectives
1.1.2 System Definition
1.1.3 List Resources Needed
1.1.4 Define System Boundary
1.1.5 Define System Components
End Define General Concerns
General Concerns [Analysis Objectives updated]
General Concerns [System Definition updated]
General Concerns [Resources list updated]
General Concerns [System boundary updated]
General Concerns [System components list updated]

STEP 1 - Define the scope of the Safety-Critical System

Subprocess-> Define general concerns

STEP 1 - Define the scope of the SCS

1.1 General Concerns

1.1.1 Analysis Objectives

The purpose of this analysis is to model an Insulin Infusion Pump (IIP) through the iterative RESafety process, generating successive refinements of the system's safety analysis artifacts.

1.1.2 System Definition

The Insulin Infusion Pump (IIP), a safety-critical system, is designed to support the treatment of Type 1 Diabetes Mellitus. Automated IIPs enhance treatment flexibility by managing multiple stages of insulin delivery, effectively mimicking physiological responses. These devices administer both rapid-acting (bolus) and continuous (basal) insulin doses.

1.1.3 Resources Needed for Analysis

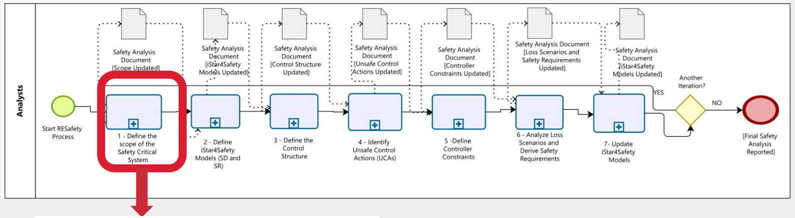
- **Articles**: Martinazzo (2022); Martins et al. (2015); Zhang et al. (2011, 2010); Bas (2020); Gonzalez Atienza et al. (2024)
- **Books**: Leveson & Thomas (2018); Martins & Gorschek (2021)
- General Guidelines and Manuals

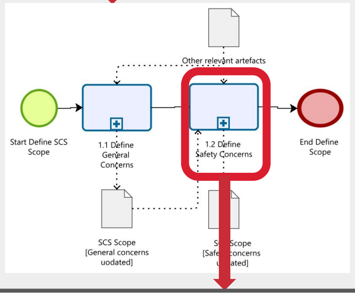
1.1.4 System Boundary

The system boundary encompasses activities from the moment the patient configures the infusion settings until the correct dosage is delivered via the catheter.

1.1.5 Components

- Patient
- Infusion Insulin Pump
- Infusion Set

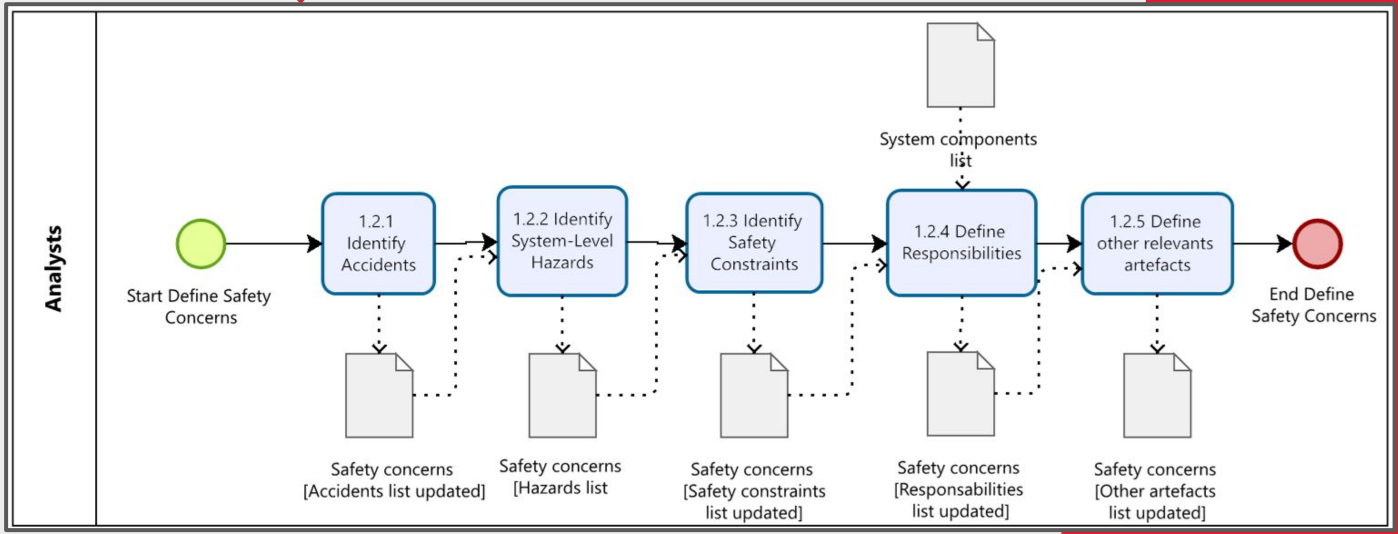

Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document [iStar4Safety Models Updated]
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]


Other relevant artefacts
Start Define SCS Scope
1.1 Define General Concerns
1.2 Define Safety Concerns
End Define Scope
SCS Scope [General concerns uodated]
S Scope [Safe concerns u ated]

RESafety

STEP 1 - Define the scope of the Safety-Critical System

Subprocess-> Define safety concerns


Analysts
Start Define Safety Concerns
1.2.1 Identify Accidents
1.2.2 Identify System-Level Hazards
1.2.3 Identify Safety Constraints
System components list
1.2.4 Define Responsibilities
1.2.5 Define other relevants artefacts
End Define Safety Concerns
Safety concerns [Accidents list updated]
Safety concerns [Hazards list
Safety concerns [Safety constraints list updated]
Safety concerns [Responsibilities list updated]
Safety concerns [Other artefacts list updated]

STEP 1 - Define the scope of the SCS

1.2 Safety Concerns

1.2.1 Identify Accidents

- **A1** - Risk of death
- **A2** - Risk of injury

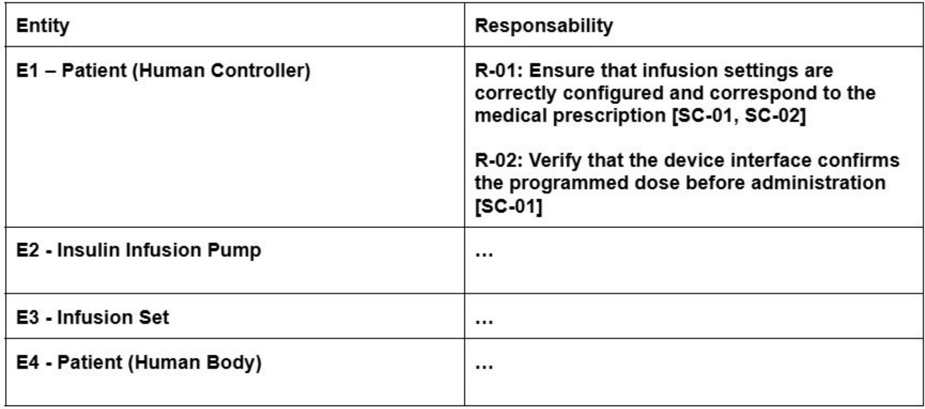
1.2.2 Identify System-Level Hazards

- **H1 -** Hypoglycemia [A1, A2]
- **H2 -** Hyperglycemia [A2]

1.2.3 Identify System Constraints

- **SC-01 -** The system must not administer insulin in excess of the prescribed dose or in unintended circumstances. [H1]
- **SC-02 -** The system must ensure that the prescribed insulin dose is delivered at the correct time and in the correct amount. [H2]

1.2.4 Identify the responsibilities



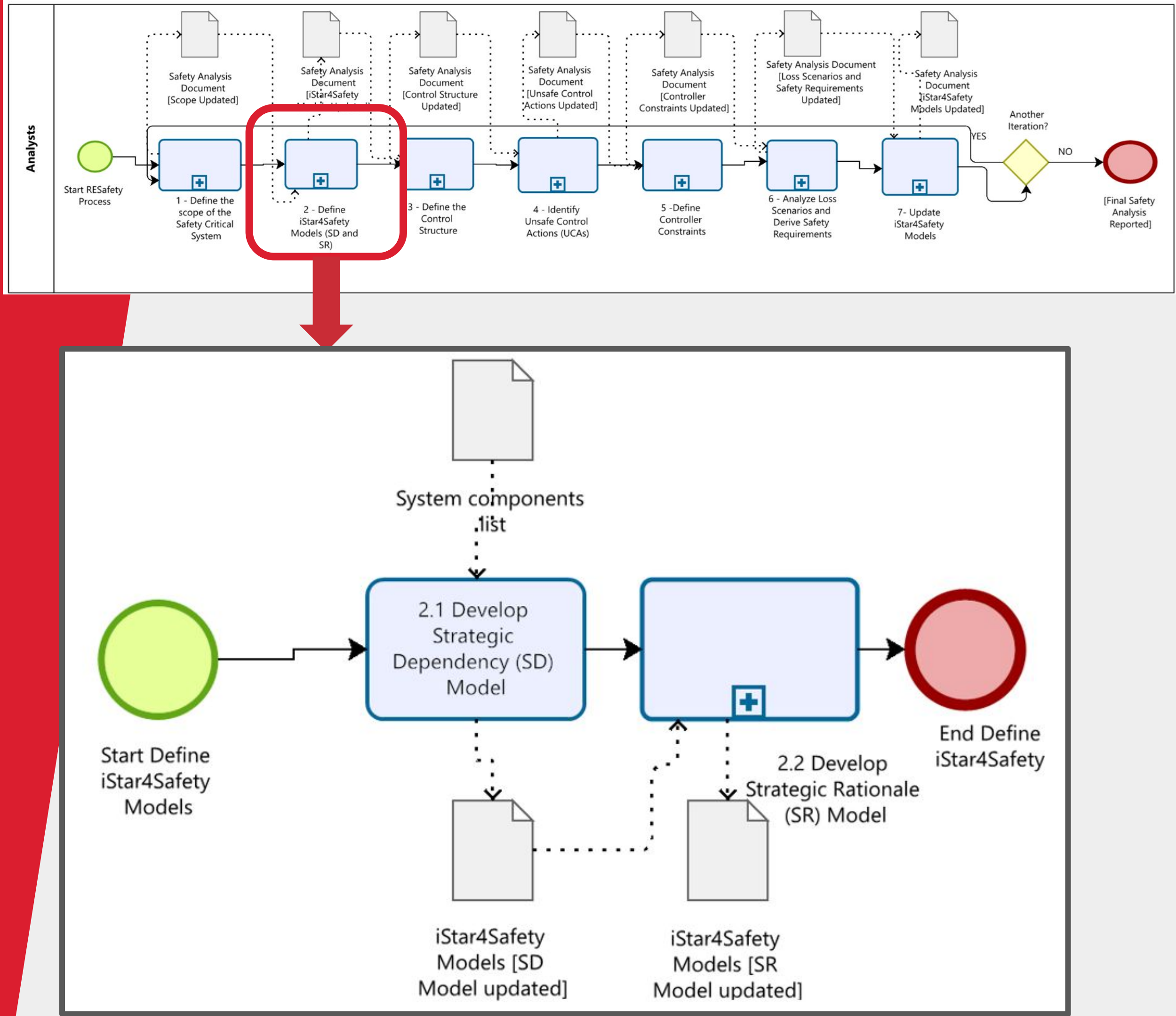
Entity	Responsability
E1 – Patient (Human Controller)	R-01: Ensure that infusion settings are correctly configured and correspond to the medical prescription [SC-01, SC-02] R-02: Verify that the device interface confirms the programmed dose before administration [SC-01]
E2 - Insulin Infusion Pump	...
E3 - Infusion Set	...
E4 - Patient (Human Body)	...

1.2.5 Other Artifacts

- *Not applicable*

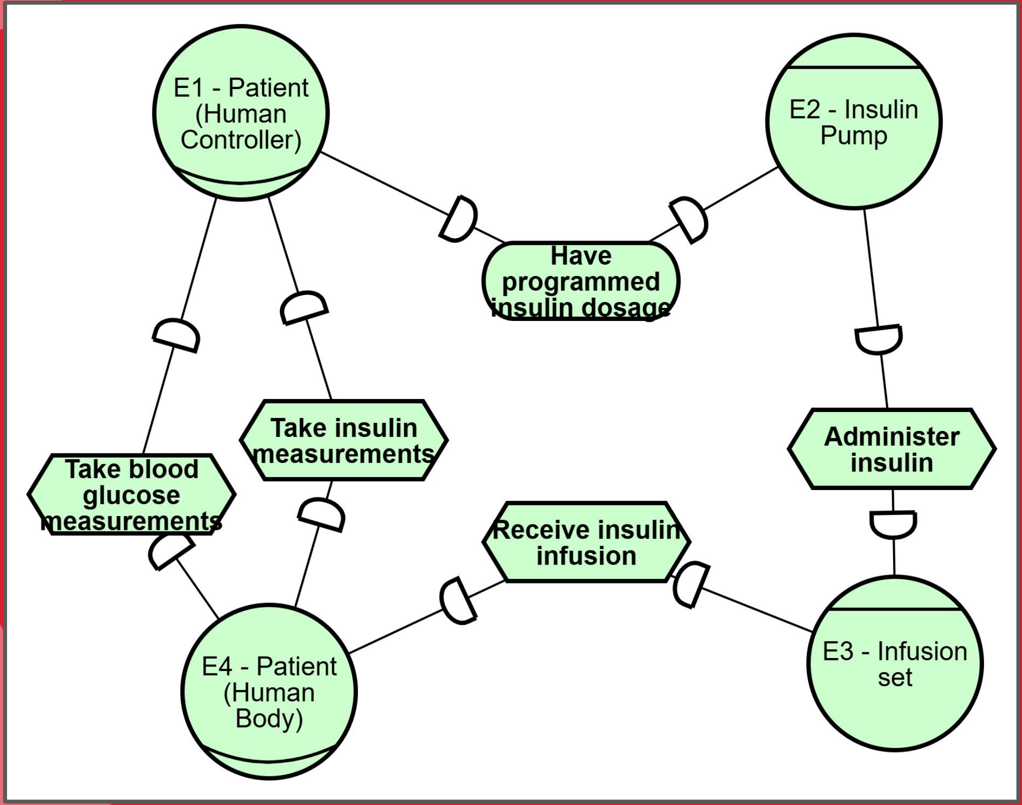
RESafety

STEP 2 - Define iStar4Safety Models (SD and SR)


Analysts
Safety Analysis Document [Scope Updated]
Safety Analysis Document [iStar4Safety
Safety Analysis Document [Control Structure Updated]
Safety Analysis Document [Unsafe Control Actions Updated]
Safety Analysis Document [Controller Constraints Updated]
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
Safety Analysis Document [iStar4Safety Models Updated]
Start RESafety Process
1 - Define the scope of the Safety Critical System
2 - Define iStar4Safety Models (SD and SR)
3 - Define the Control Structure
4 - Identify Unsafe Control Actions (UCAs)
5 -Define Controller Constraints
6 - Analyze Loss Scenarios and Derive Safety Requirements
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]
System components list
Start Define iStar4Safety Models
2.1 Develop Strategic Dependency (SD) Model
2.2 Develop Strategic Rationale (SR) Model
End Define iStar4Safety
iStar4Safety Models [SD Model updated]
iStar4Safety Models [SR Model updated]

STEP 2 - Define iStar4Safety Models

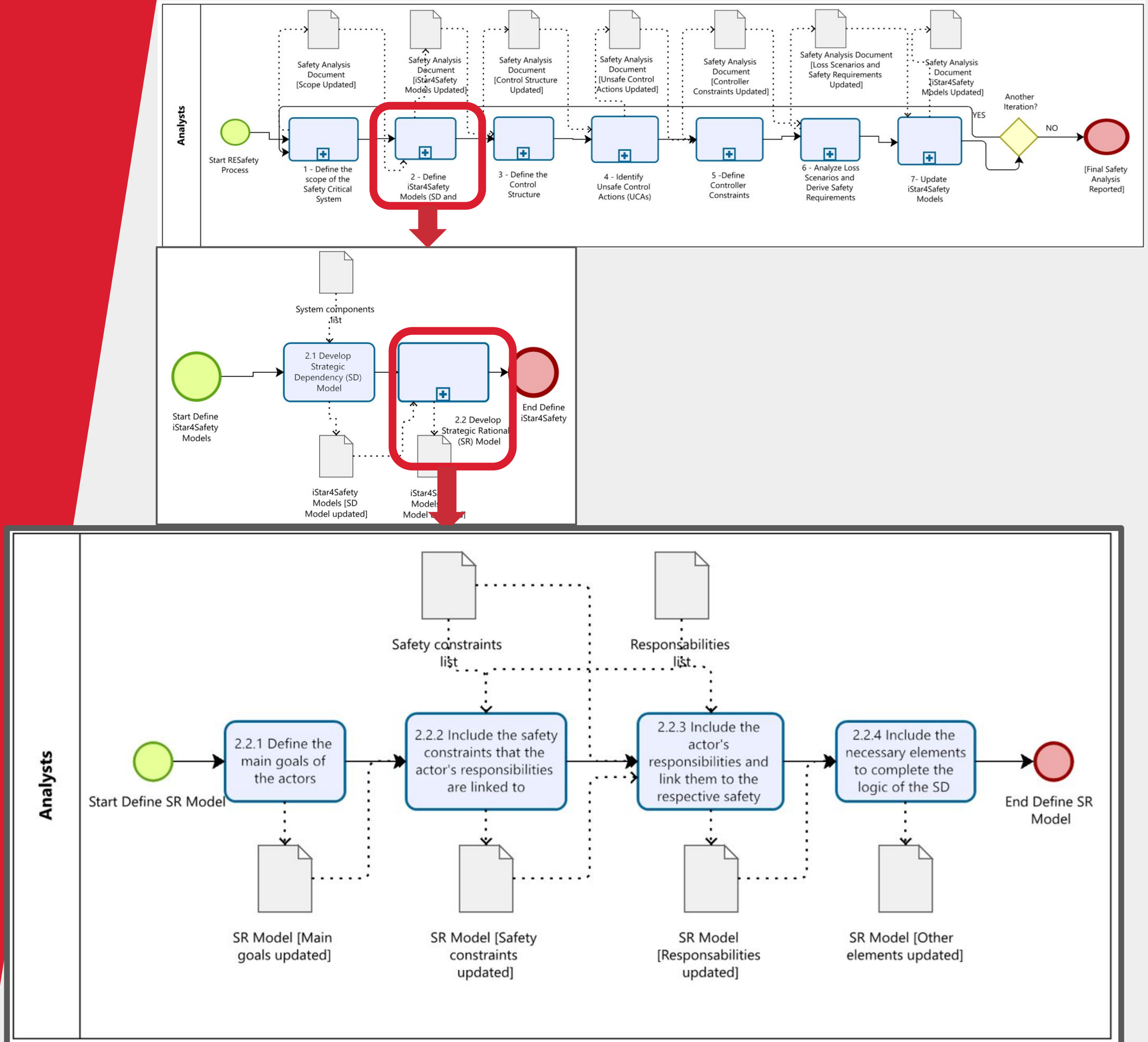
SD Model


E1 - Patient (Human Controller)
E2 - Insulin Pump
Have programmed insulin dosage
Take insulin measurements
Take blood glucose measurements
Administer insulin
Receive insulin infusion
E4 - Patient (Human Body)
E3 - Infusion set

RESafety

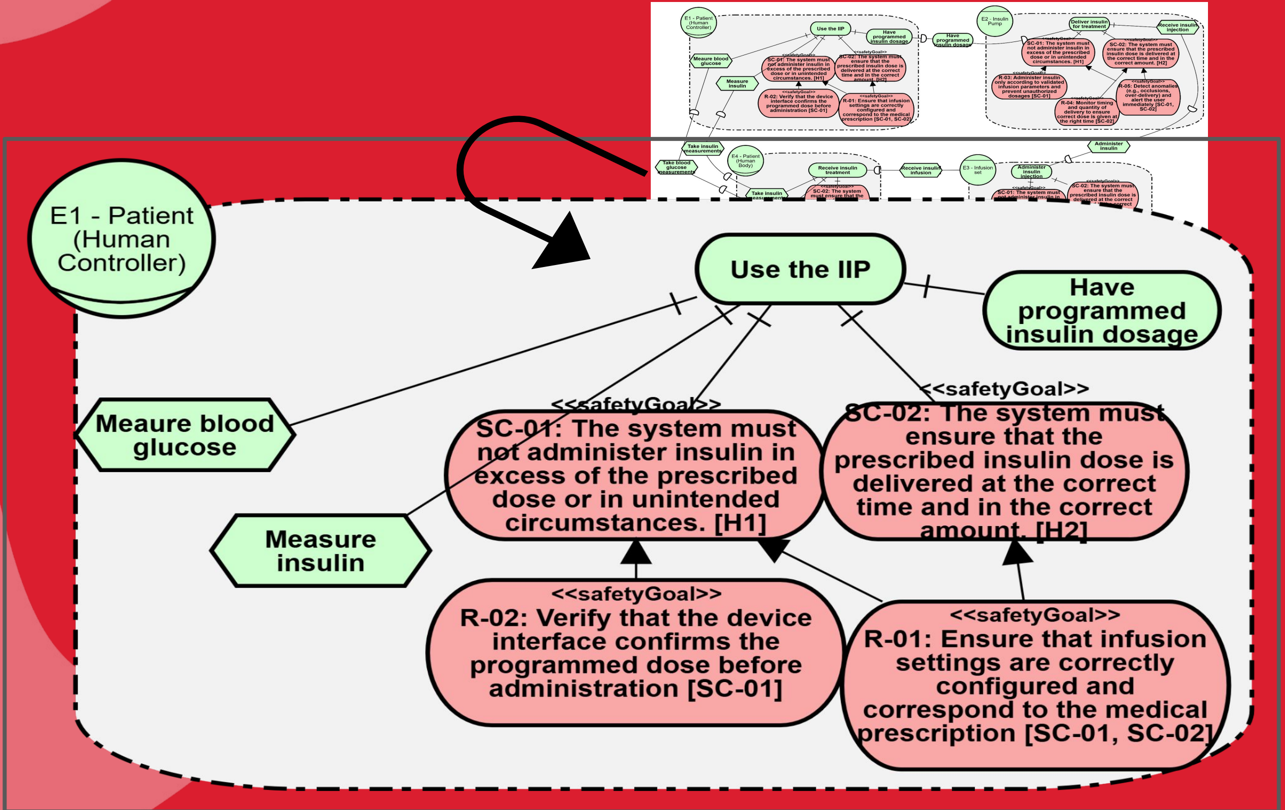
STEP 2 - Define iStar4Safety Models (SD and SR) -

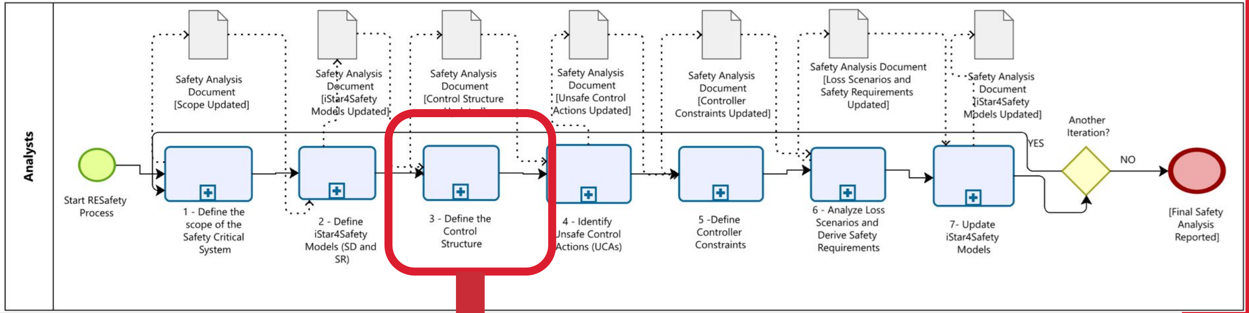
Subprocess-> Develop Strategic Rationale (SR) model


Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document [iStar4Safety Models Updated]
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]
System components list
Start Define iStar4Safety Models
2.1 Develop Strategic Dependency (SD) Model
2.2 Develop Strategic Rational (SR) Model
End Define iStar4Safety
iStar4Safety Models [SD Model updated]
iStar4S Models Model
Analysts
Safety constraints list
Responsabilities list
Start Define SR Model
2.2.1 Define the main goals of the actors
2.2.2 Include the safety constraints that the actor's responsibilities are linked to
2.2.3 Include the actor's responsibilities and link them to the respective safety
2.2.4 Include the necessary elements to complete the logic of the SD
End Define SR Model
SR Model [Main goals updated]
SR Model [Safety constraints updated]
SR Model [Responsabilities updated]
SR Model [Other elements updated]

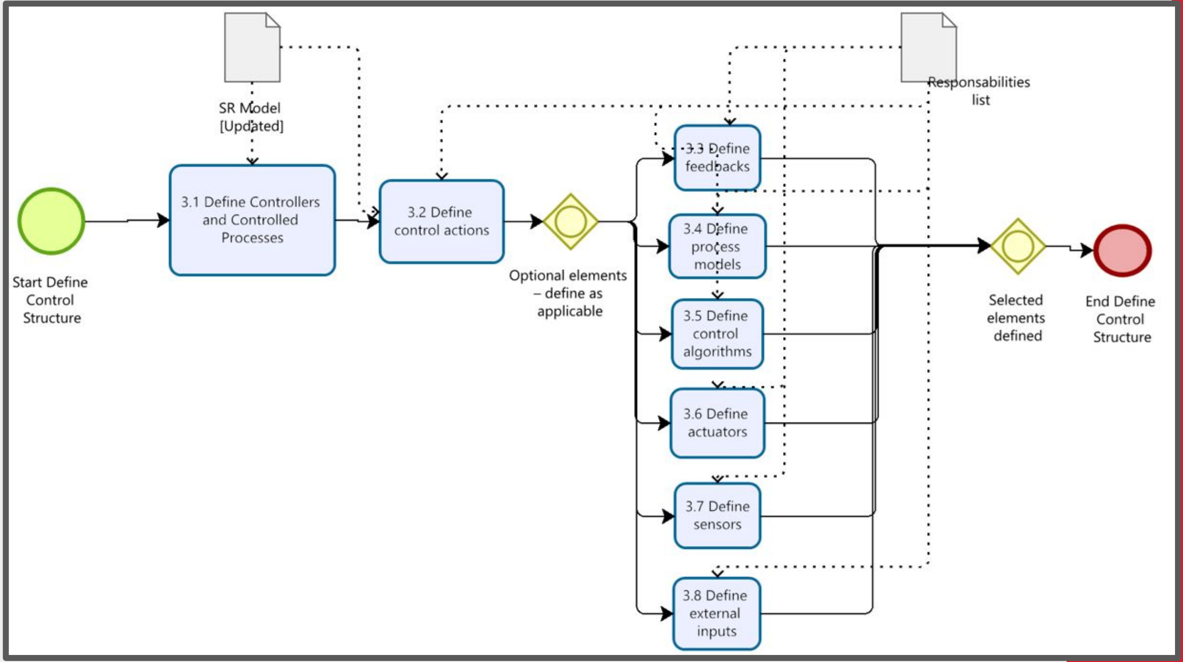
STEP 2 - Define iStar4Safety Models

SD and SR Models


E1 - Patient (Human Controller)
Use the IIP
Have programmed insulin dosage
Meaure blood glucose
Measure insulin
<<safetyGoal>>
SC-01: The system must not administer insulin in excess of the prescribed dose or in unintended circumstances. [H1]
<<safetyGoal>>
SC-02: The system must ensure that the prescribed insulin dose is delivered at the correct time and in the correct amount. [H2]
<<safetyGoal>>
R-02: Verify that the device interface confirms the programmed dose before administration [SC-01]
<<safetyGoal>>
R-01: Ensure that infusion settings are correctly configured and correspond to the medical prescription [SC-01, SC-02]
E2 - Insulin Pump
Deliver insulin for treatment
Receive insulin injection
R-03: Administer insulin only according to validated infusion parameters and prevent unauthorized dosages [SC-01]
R-04: Monitor timing and quantity of delivery to ensure correct dose is given at the right time [SC-02]
R-05: Detect anomalies (e.g., occlusions, over-delivery) and alert the user immediately [SC-01, SC-02]
Take insulin measurements
Take blood glucose measurements
E4 - Patient (Human Body)
Receive insulin treatment
Receive insulin infusion
E3 - Infusion set
Administer insulin injection
Administer insulin

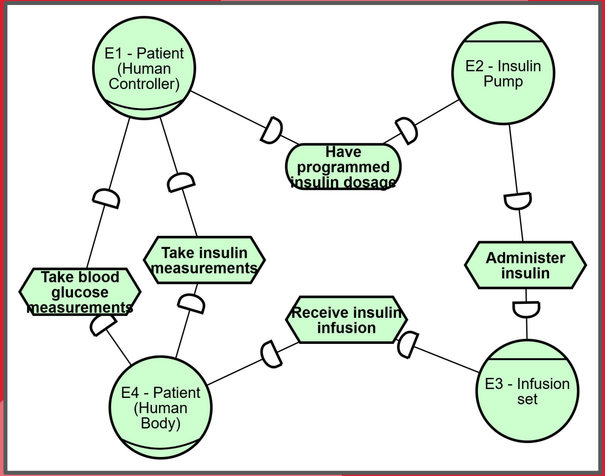

Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document iStar4Safety Models Updated]
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]

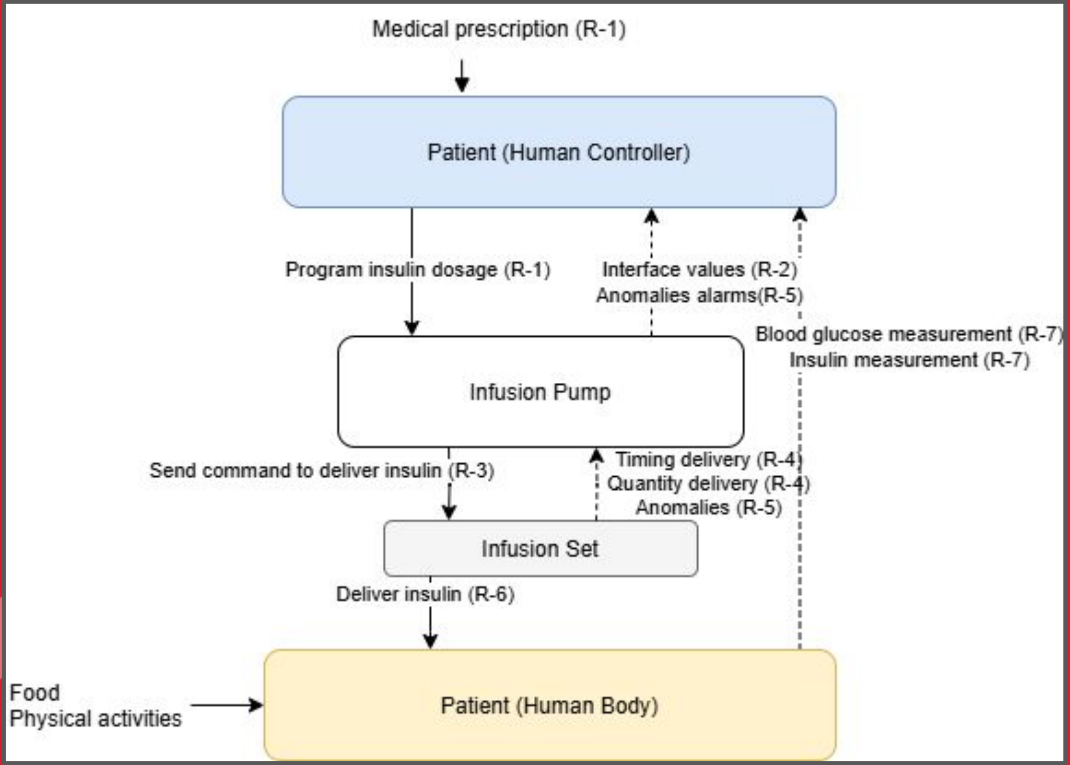
RESafety


SR Model [Updated]
Responsabilities list
Start Define Control Structure
3.1 Define Controllers and Controlled Processes
3.2 Define control actions
Optional elements – define as applicable
3.3 Define feedbacks
3.4 Define process models
3.5 Define control algorithms
3.6 Define actuators
3.7 Define sensors
3.8 Define external inputs
Selected elements defined
End Define Control Structure

STEP 3 - Define the Control Structure

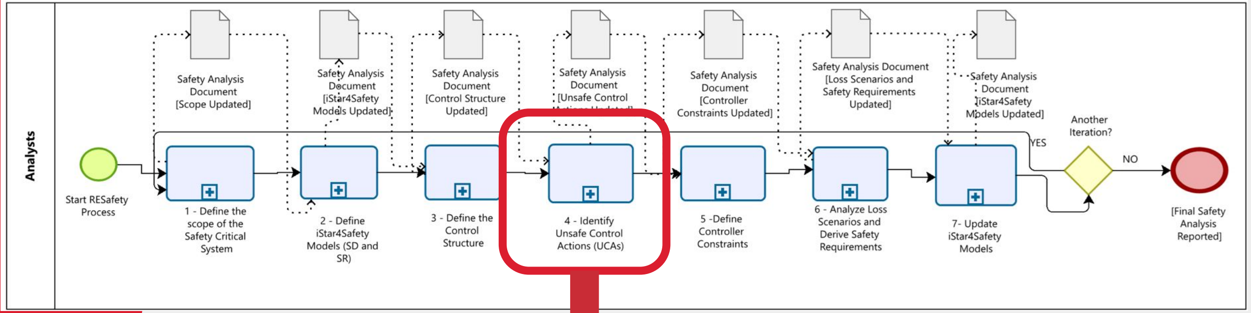
STEP 3 - Define the Control Structure

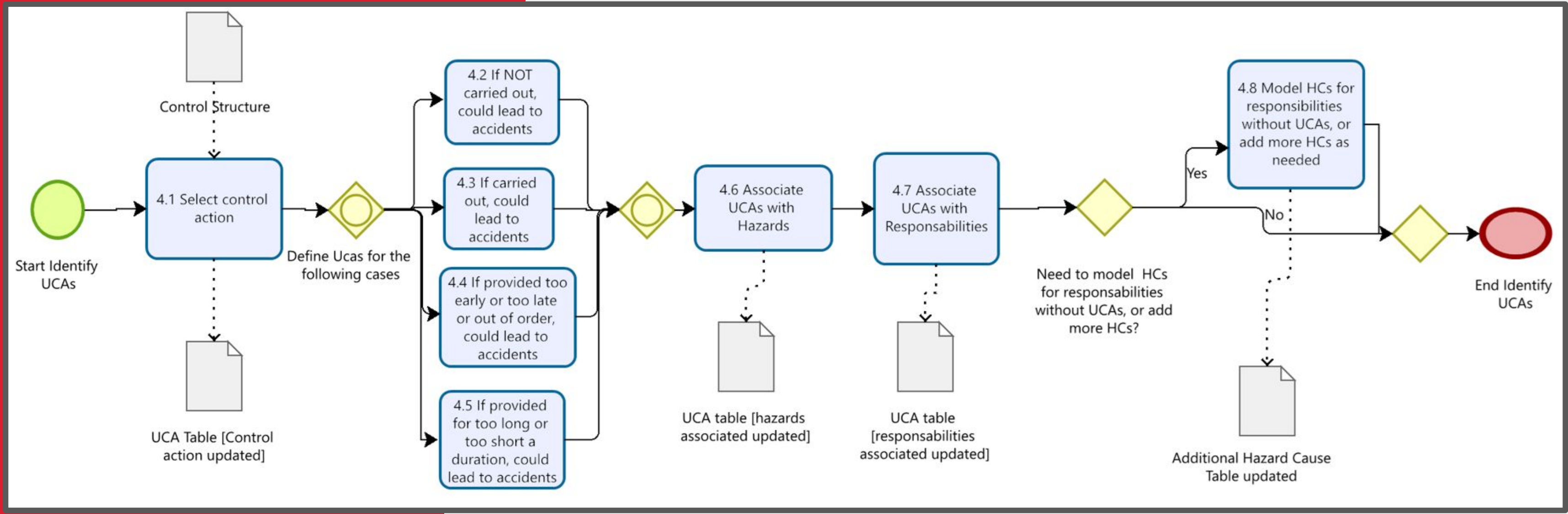

E1 - Patient (Human Controller)
E2 - Insulin Pump
Have programmed insulin dosage
Take insulin measurements
Administer insulin
Take blood glucose measurements
Receive insulin infusion
E4 - Patient (Human Body)
E3 - Infusion set



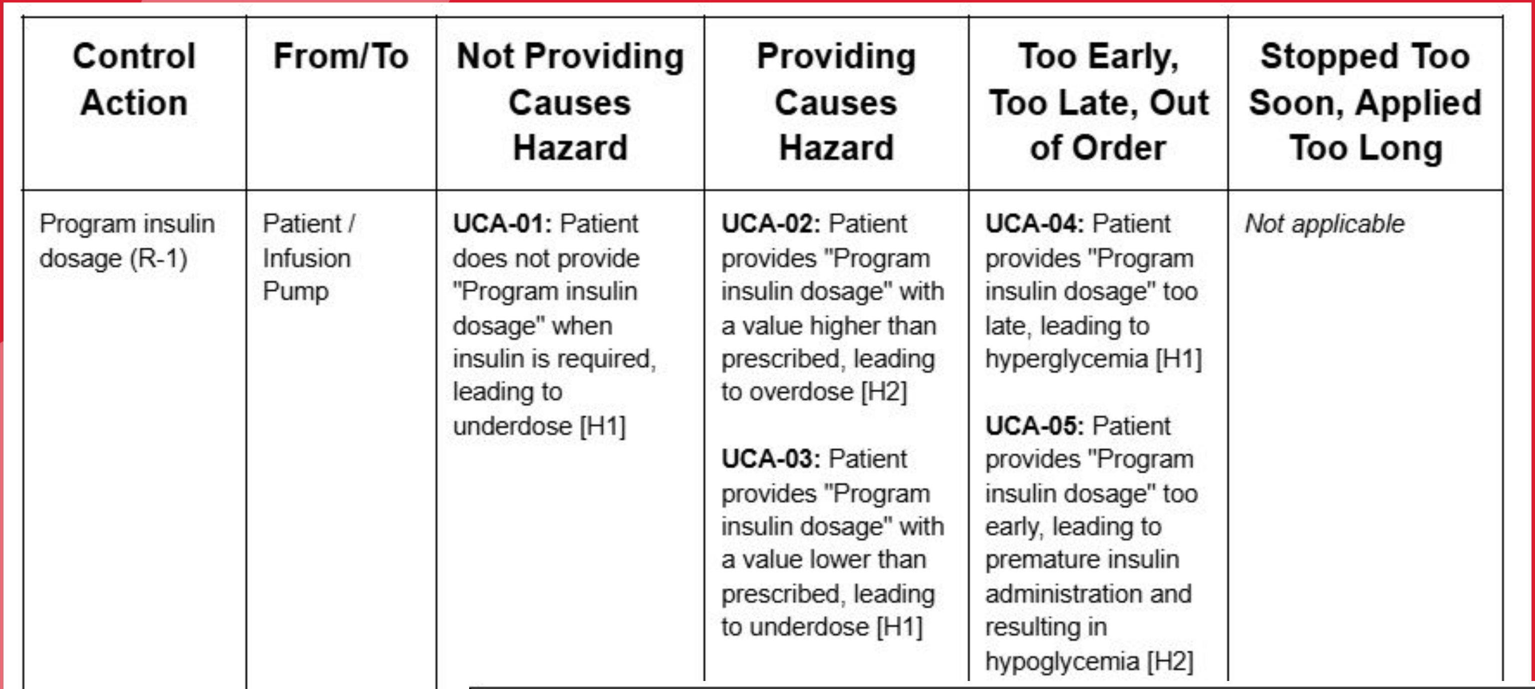
RESafety

STEP 4 - Identify Unsafe Control Actions (UCAs)

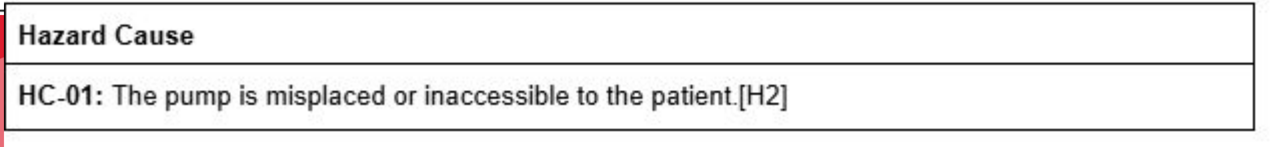

Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document [iStar4Safety Models Updated]
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]


Start Identify UCAs
Control Structure
4.1 Select control action
UCA Table [Control action updated]
Define Ucas for the following cases
4.2 If NOT carried out, could lead to accidents
4.3 If carried out, could lead to accidents
4.4 If provided too early or too late or out of order, could lead to accidents
4.5 If provided for too long or too short a duration, could lead to accidents
4.6 Associate UCAs with Hazards
UCA table [hazards associated updated]
4.7 Associate UCAs with Responsabilities
UCA table [responsabilities associated updated]
Need to model HCs for responsabilities without UCAs, or add more HCs?
Yes
No
4.8 Model HCs for responsibilities without UCAs, or add more HCs as needed
Additional Hazard Cause Table updated
End Identify UCAs

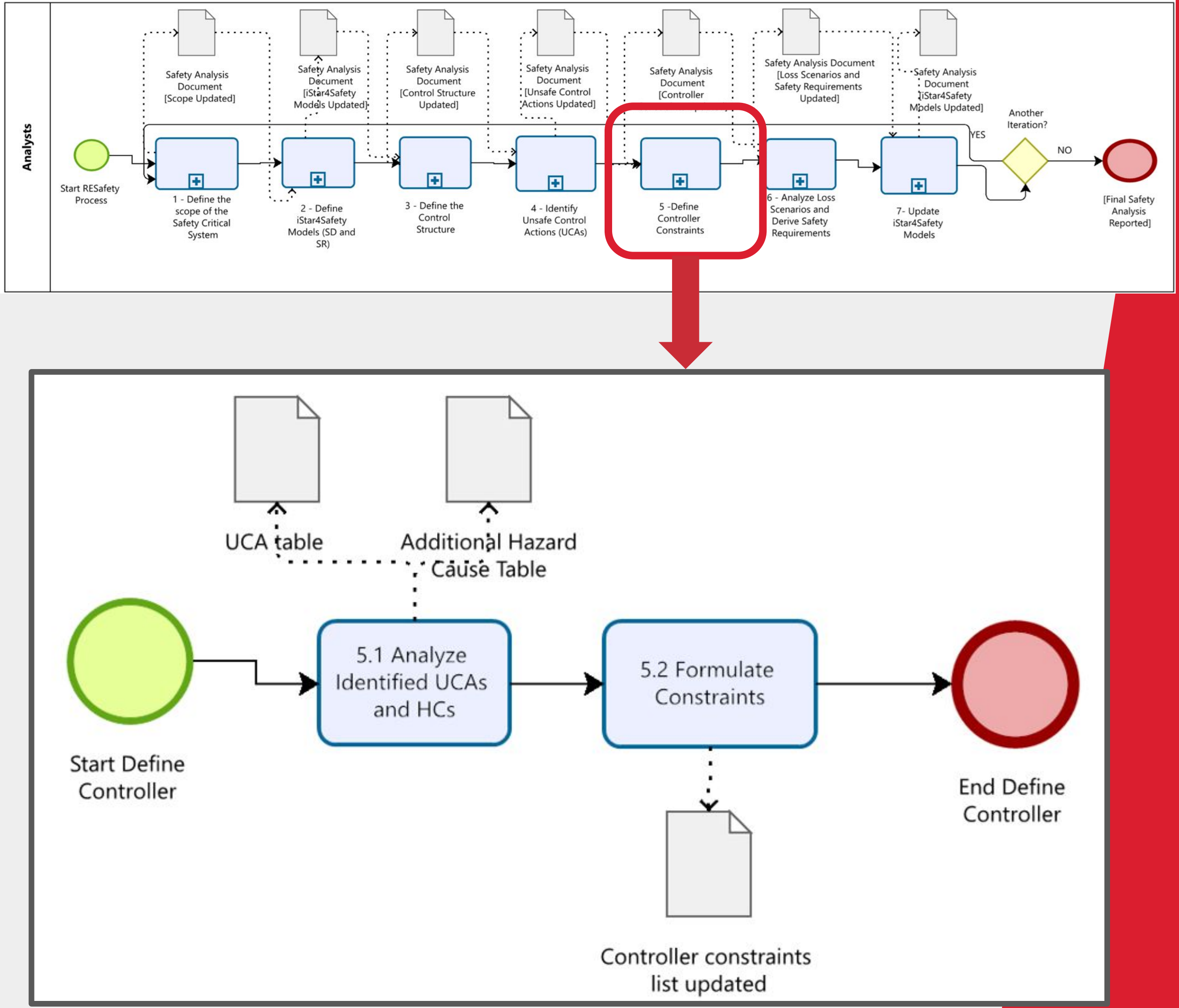
STEP 4 - Define UCAs



Control Action	From/To	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped Too Soon, Applied Too Long
Program insulin dosage (R-1)	Patient / Infusion Pump	**UCA-01:** Patient does not provide "Program insulin dosage" when insulin is required, leading to underdose [H1]	**UCA-02:** Patient provides "Program insulin dosage" with a value higher than prescribed, leading to overdose [H2] **UCA-03:** Patient provides "Program insulin dosage" with a value lower than prescribed, leading to underdose [H1]	**UCA-04:** Patient provides "Program insulin dosage" too late, leading to hyperglycemia [H1] **UCA-05:** Patient provides "Program insulin dosage" too early, leading to premature insulin administration and resulting in hypoglycemia [H2]	*Not applicable*



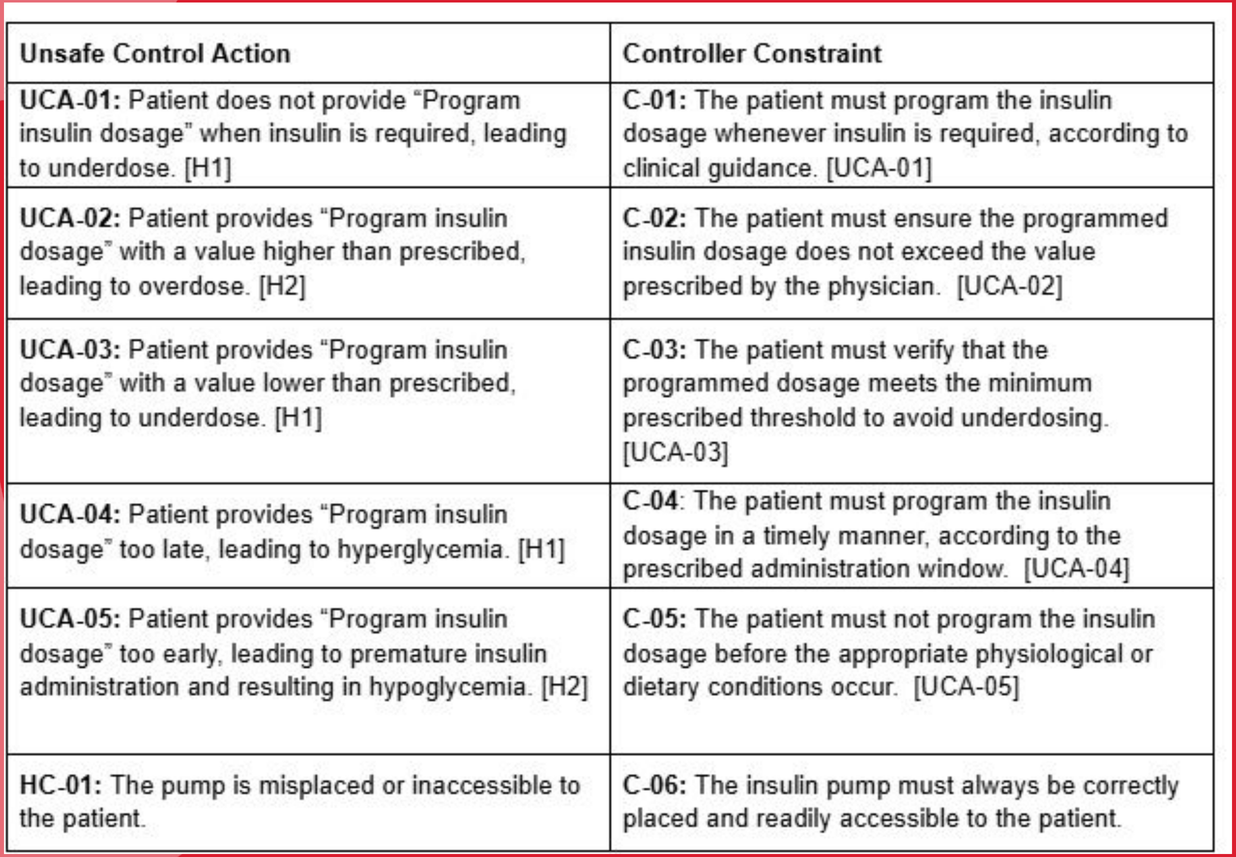
Hazard Cause
HC-01: The pump is misplaced or inaccessible to the patient.[H2]


Analysts
Safety Analysis Document [Scope Updated]
Safety Analysis Document [iStar4Safety Models Updated]
Safety Analysis Document [Control Structure Updated]
Safety Analysis Document [Unsafe Control Actions Updated]
Safety Analysis Document [Controller
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
Safety Analysis Document [iStar4Safety Models Updated]
Another Iteration?
YES
NO
Start RESafety Process
1 - Define the scope of the Safety Critical System
2 - Define iStar4Safety Models (SD and SR)
3 - Define the Control Structure
4 - Identify Unsafe Control Actions (UCAs)
5 -Define Controller Constraints
6 - Analyze Loss Scenarios and Derive Safety Requirements
7- Update iStar4Safety Models
[Final Safety Analysis Reported]
UCA table
Additional Hazard Cause Table
Start Define Controller
5.1 Analyze Identified UCAs and HCs
5.2 Formulate Constraints
End Define Controller
Controller constraints list updated

RESafety

STEP 5 -
Define controller constraints

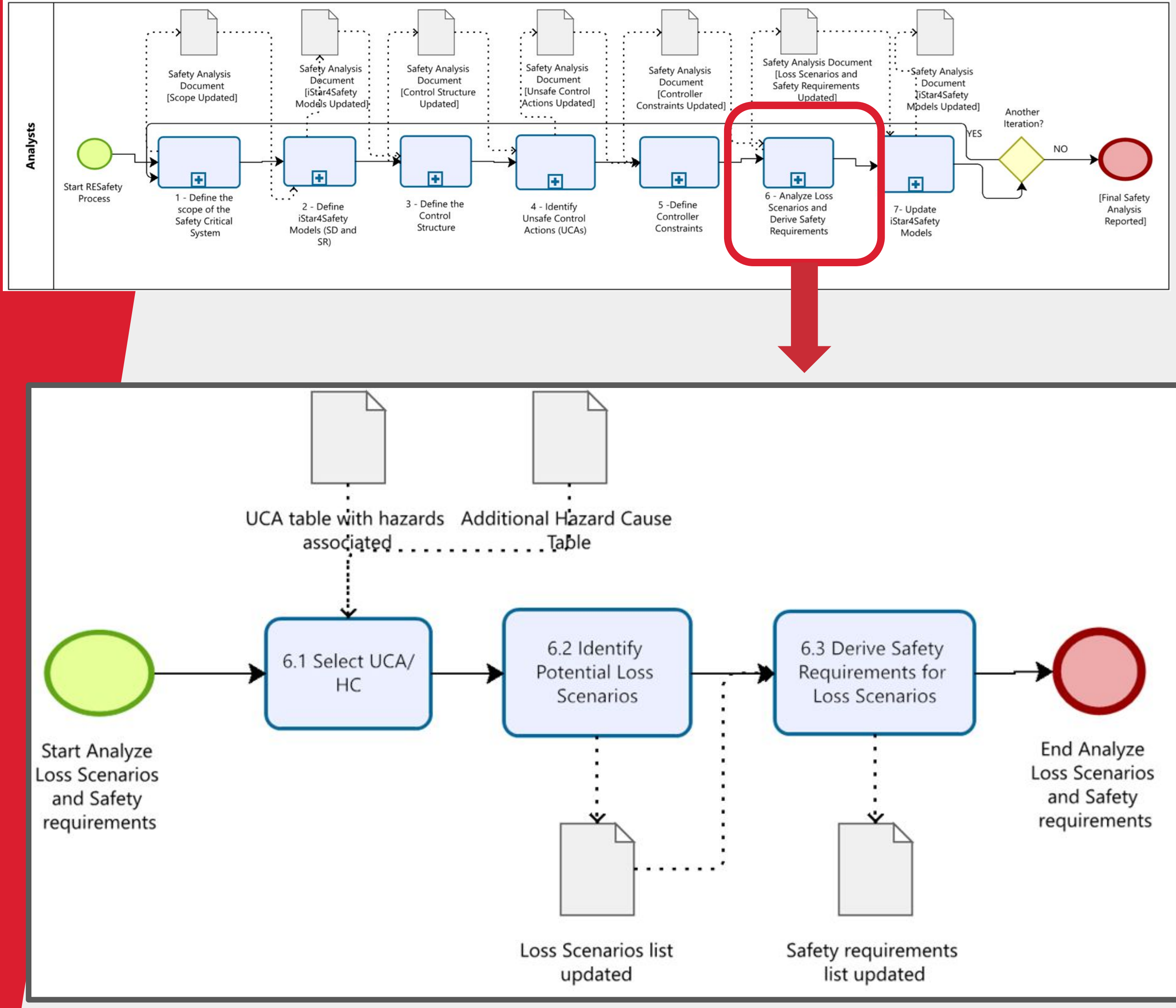
STEP 5 - Define Controller Constraints



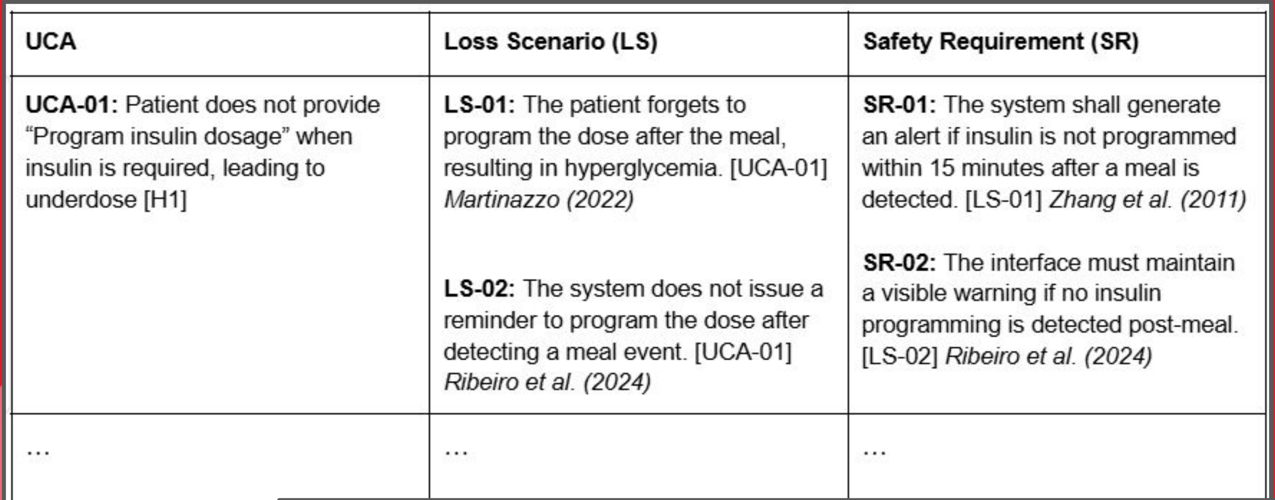
Unsafe Control Action	Controller Constraint
UCA-01: Patient does not provide "Program insulin dosage" when insulin is required, leading to underdose. [H1]	**C-01:** The patient must program the insulin dosage whenever insulin is required, according to clinical guidance. [UCA-01]
UCA-02: Patient provides "Program insulin dosage" with a value higher than prescribed, leading to overdose. [H2]	**C-02:** The patient must ensure the programmed insulin dosage does not exceed the value prescribed by the physician. [UCA-02]
UCA-03: Patient provides "Program insulin dosage" with a value lower than prescribed, leading to underdose. [H1]	**C-03:** The patient must verify that the programmed dosage meets the minimum prescribed threshold to avoid underdosing. [UCA-03]
UCA-04: Patient provides "Program insulin dosage" too late, leading to hyperglycemia. [H1]	**C-04**: The patient must program the insulin dosage in a timely manner, according to the prescribed administration window. [UCA-04]
UCA-05: Patient provides "Program insulin dosage" too early, leading to premature insulin administration and resulting in hypoglycemia. [H2]	**C-05:** The patient must not program the insulin dosage before the appropriate physiological or dietary conditions occur. [UCA-05]
HC-01: The pump is misplaced or inaccessible to the patient.	**C-06:** The insulin pump must always be correctly placed and readily accessible to the patient.

RESafety

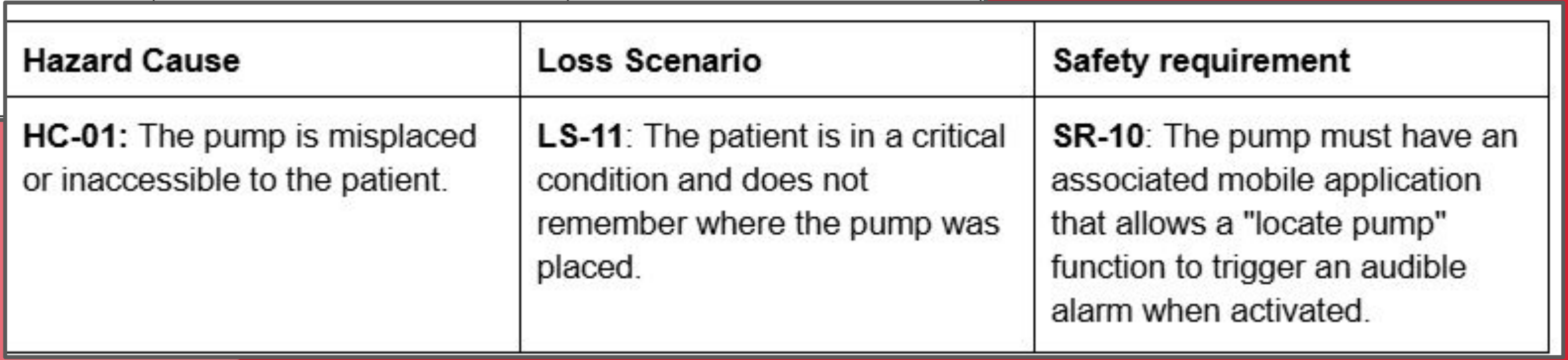
STEP 6 - Analyze Loss Scenarios and derive safety requirements


Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document [iStar4Safety Models Updated]
7- Update iStar4Safety Models
Another Iteration?
YES
NO
[Final Safety Analysis Reported]
UCA table with hazards associated
Additional Hazard Cause Table
Start Analyze Loss Scenarios and Safety requirements
6.1 Select UCA/ HC
6.2 Identify Potential Loss Scenarios
6.3 Derive Safety Requirements for Loss Scenarios
End Analyze Loss Scenarios and Safety requirements
Loss Scenarios list updated
Safety requirements list updated

STEP 6 - Analyze Loss Scenarios and derive safety requirements



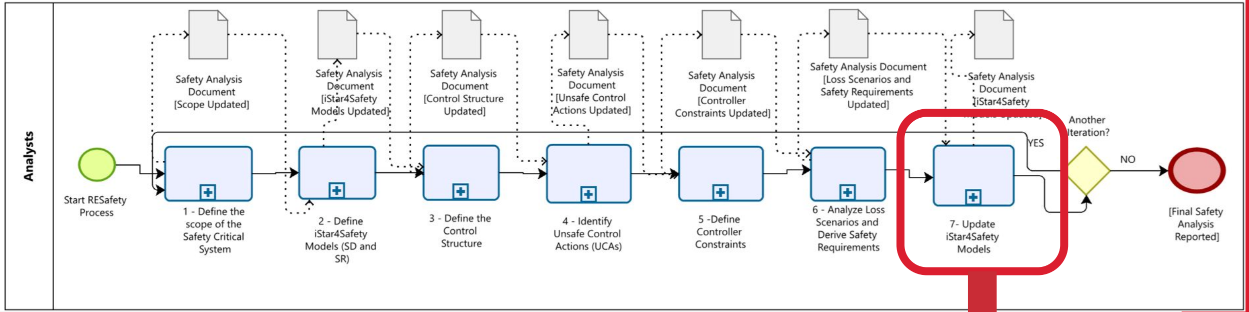
UCA	Loss Scenario (LS)	Safety Requirement (SR)
UCA-01: Patient does not provide “Program insulin dosage” when insulin is required, leading to underdose [H1]	**LS-01:** The patient forgets to program the dose after the meal, resulting in hyperglycemia. [UCA-01] *Martinazzo (2022)* **LS-02:** The system does not issue a reminder to program the dose after detecting a meal event. [UCA-01] *Ribeiro et al. (2024)*	**SR-01:** The system shall generate an alert if insulin is not programmed within 15 minutes after a meal is detected. [LS-01] *Zhang et al. (2011)* **SR-02:** The interface must maintain a visible warning if no insulin programming is detected post-meal. [LS-02] *Ribeiro et al. (2024)*
...	...	...



Hazard Cause	Loss Scenario	Safety requirement
HC-01: The pump is misplaced or inaccessible to the patient.	**LS-11**: The patient is in a critical condition and does not remember where the pump was placed.	**SR-10**: The pump must have an associated mobile application that allows a "locate pump" function to trigger an audible alarm when activated.

RESafety

STEP 7 -
Update iStar4Safety Models



Analysts

Start RESafety Process

Safety Analysis Document [Scope Updated]

1 - Define the scope of the Safety Critical System

Safety Analysis Document [iStar4Safety Models Updated]

2 - Define iStar4Safety Models (SD and SR)

Safety Analysis Document [Control Structure Updated]

3 - Define the Control Structure

Safety Analysis Document [Unsafe Control Actions Updated]

4 - Identify Unsafe Control Actions (UCAs)

Safety Analysis Document [Controller Constraints Updated]

5 -Define Controller Constraints

Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]

6 - Analyze Loss Scenarios and Derive Safety Requirements

Safety Analysis Document iStar4Safety Models Updated]

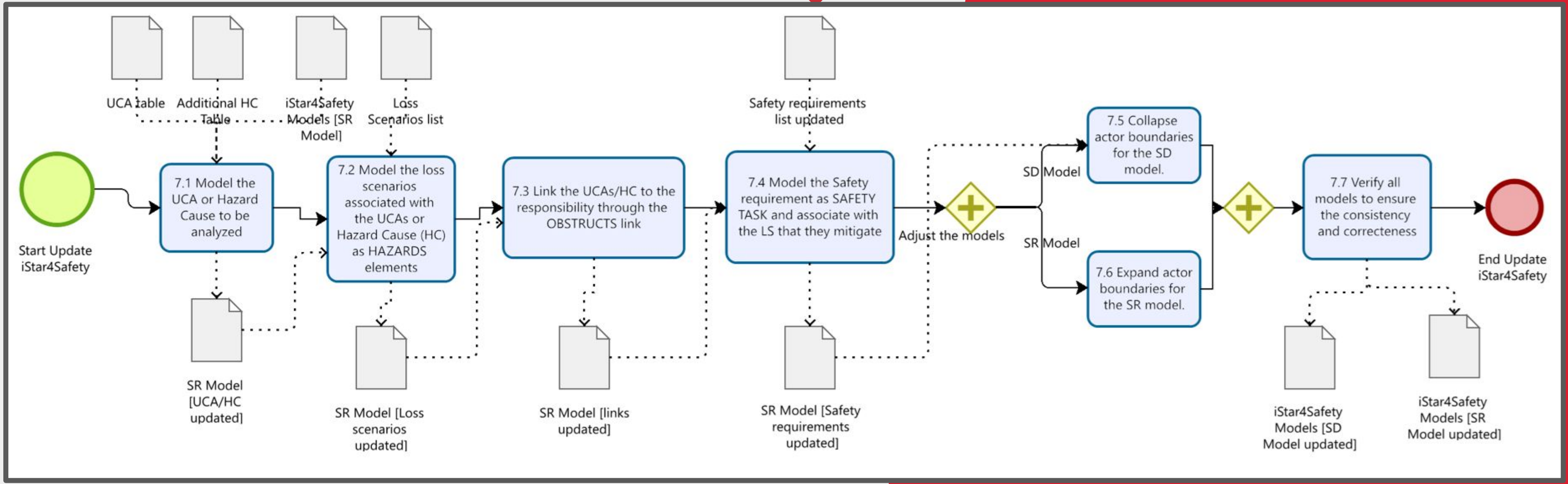
7- Update iStar4Safety Models

Another Iteration?

YES

NO

[Final Safety Analysis Reported]



Start Update iStar4Safety

UCA table

Additional HC Table

iStar4Safety Models [SR Model]

Loss Scenarios list

7.1 Model the UCA or Hazard Cause to be analyzed

SR Model [UCA/HC updated]

7.2 Model the loss scenarios associated with the UCAs or Hazard Cause (HC) as HAZARDS elements

SR Model [Loss scenarios updated]

7.3 Link the UCAs/HC to the responsibility through the OBSTRUCTS link

SR Model [links updated]

Safety requirements list updated

7.4 Model the Safety requirement as SAFETY TASK and associate with the LS that they mitigate

SR Model [Safety requirements updated]

Adjust the models

SD Model

SR Model

7.5 Collapse actor boundaries for the SD model.

7.6 Expand actor boundaries for the SR model.

7.7 Verify all models to ensure the consistency and correctness

iStar4Safety Models [SD Model updated]

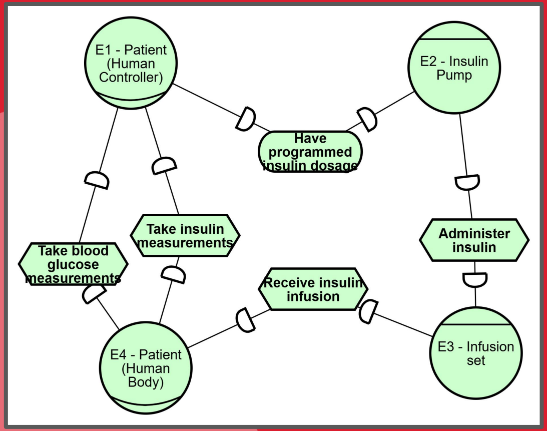
iStar4Safety Models [SR Model updated]

End Update iStar4Safety

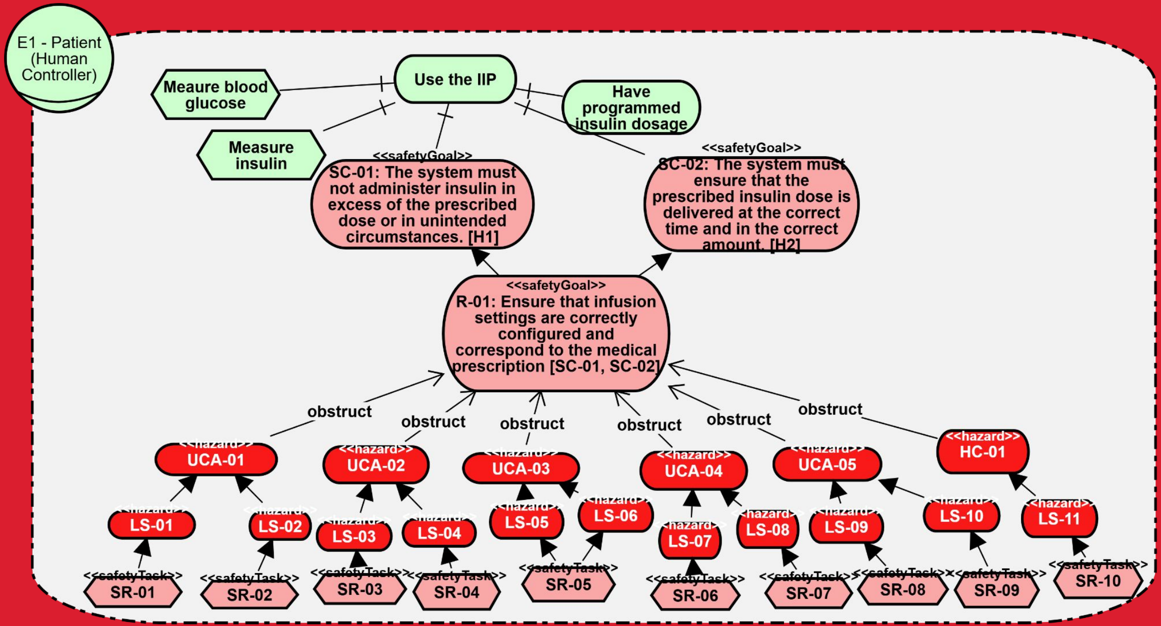
STEP 7 - Update iStar4Safety Models

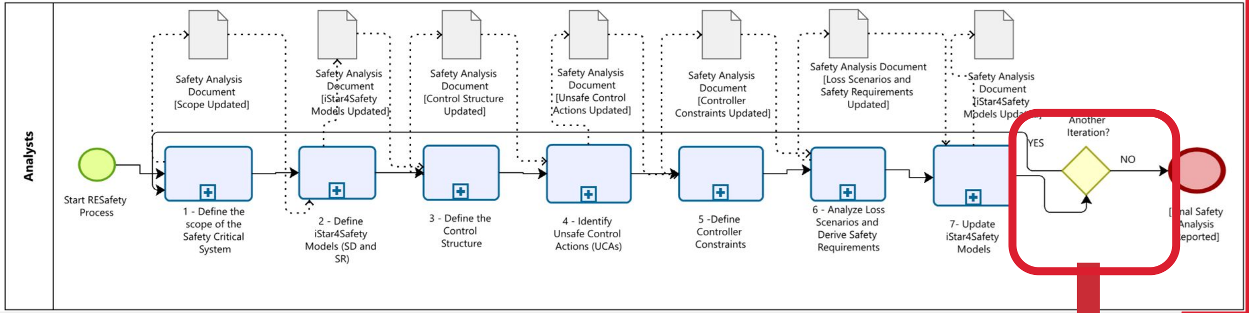
SD and SR Model

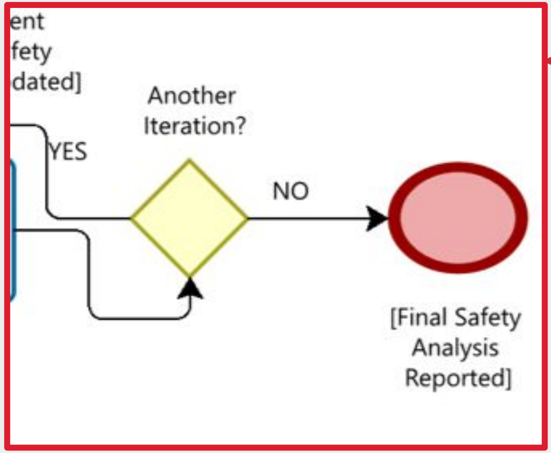
7.1 SD Model (The same)


E1 - Patient (Human Controller)
E2 - Insulin Pump
Have programmed insulin dosage
Take insulin measurements
Administer insulin
Take blood glucose measurements
Receive insulin infusion
E4 - Patient (Human Body)
E3 - Infusion set

7.2 SR Model




Analysts
Start RESafety Process
Safety Analysis Document [Scope Updated]
1 - Define the scope of the Safety Critical System
Safety Analysis Document [iStar4Safety Models Updated]
2 - Define iStar4Safety Models (SD and SR)
Safety Analysis Document [Control Structure Updated]
3 - Define the Control Structure
Safety Analysis Document [Unsafe Control Actions Updated]
4 - Identify Unsafe Control Actions (UCAs)
Safety Analysis Document [Controller Constraints Updated]
5 -Define Controller Constraints
Safety Analysis Document [Loss Scenarios and Safety Requirements Updated]
6 - Analyze Loss Scenarios and Derive Safety Requirements
Safety Analysis Document iStar4Safety Models Upda
7- Update iStar4Safety Models
Another Iteration?
YES
NO
nal Safety Analysis eported]



RESafety

“Another iteration” Exclusive Gateway

Vs

“Final Safety Analysis Reported” End Event

References

1. A. Martinazzo, L. E. G. Martins, S. V. Aredes and T. S. Cunha, "Risk Management of a Low-cost Insulin Infusion Pump: A Case Study with a Brazilian Company," 2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS), Aveiro, Portugal, 2021.
2. WikEM. (n.d.). Insulin infusion device complication. Retrieved June 3, 2025, from http://medbox.iiab.me/modules/en-wikem/wiki/Insulin_infusion_device_complication.html

Thanks!

Contacts:

Moniky Ribeiro-> monikyr@gmail.com **or**
smsr@cin.ufpe.br

Jaelson Castro-> jbc@cin.ufpe.br