RESafety Analysis
Insulin Infusion System

Author: Moniky Ribeiro
Date: June 2025
Project or Institute: CIn/UFPE
System: Insulin Infusion Pump (IIP)
Iteration: 1ª

Step 1 - Define Safety-Critical System (SCS) Scope

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

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 Define 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	**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]

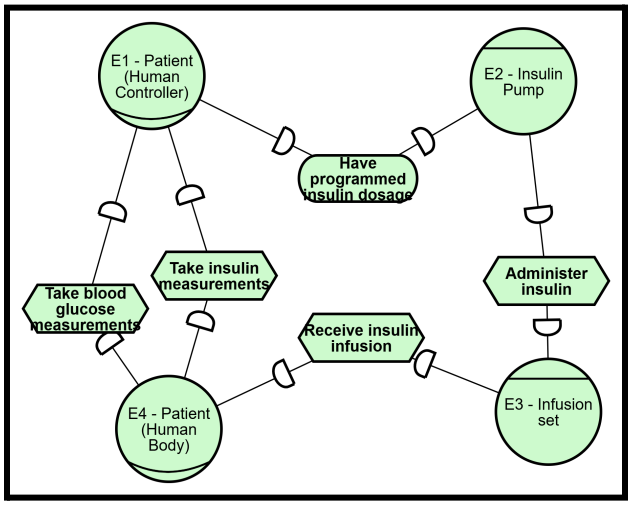
E3 - Infusion Set	**R-06:** Maintain physical integrity to prevent leaks or unintended flow of insulin [SC-01] **R-07:** Ensure correct and timely delivery of insulin from pump to patient [SC-02]
E4 - Patient (Human Body)	**R-08:** Respond physiologically to insulin in a way that is consistent with treatment expectations (acknowledging variability) [SC-02]

1.2.5. Other Artifacts

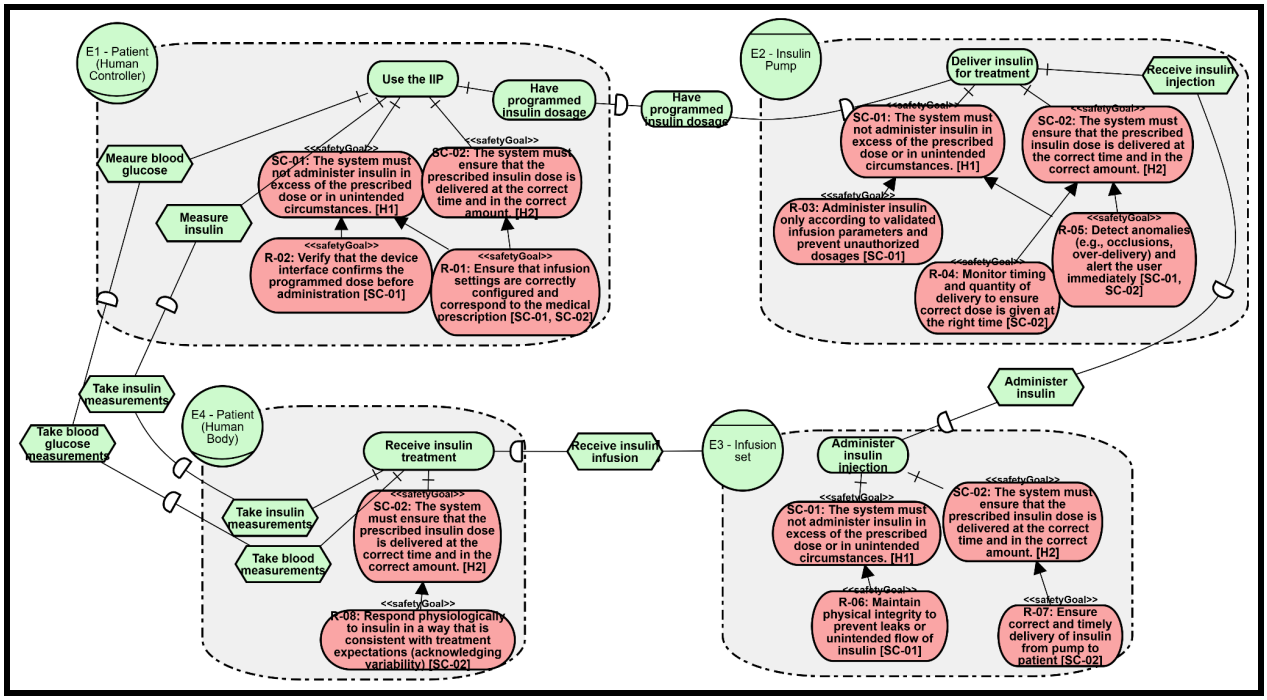
- *Not applicable*

Step 2 - Define the iStar4Safety Models

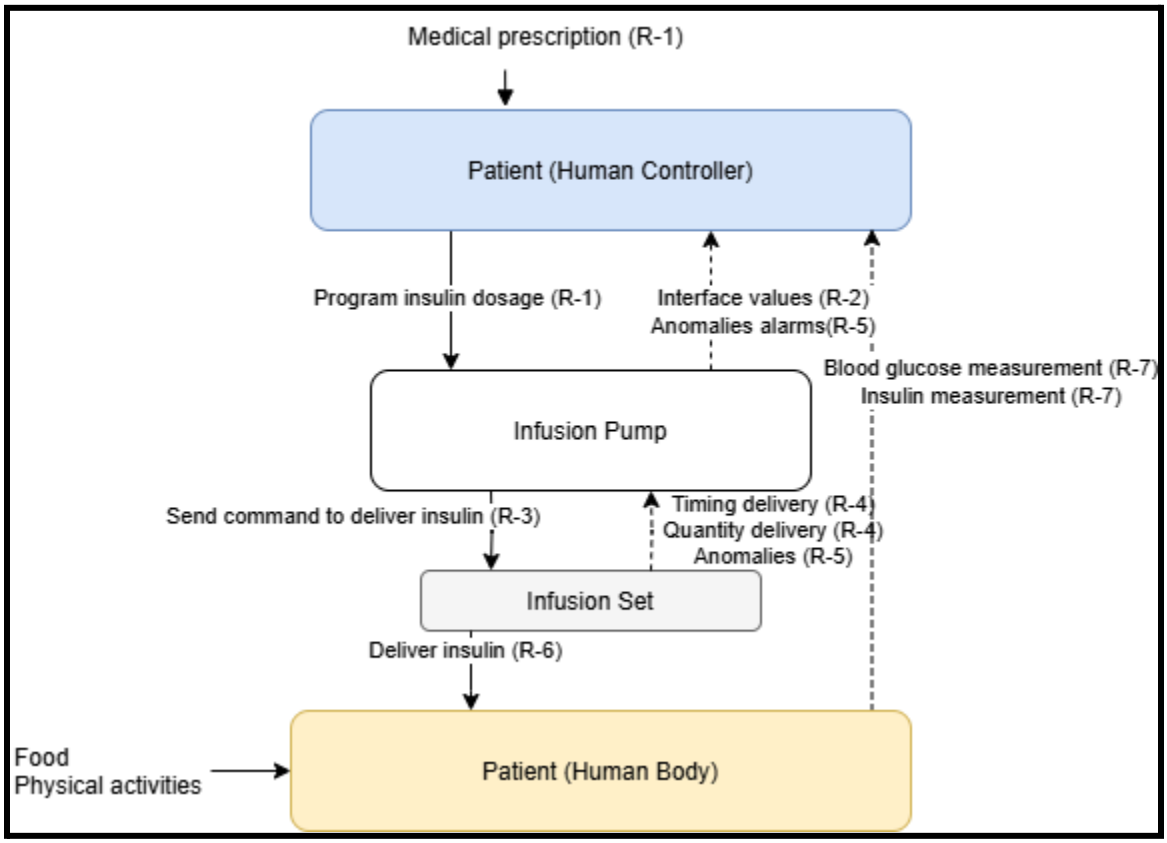
- **SD Model**



- **SR Model**


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]
Have programmed insulin dosage
E2 - Insulin Pump
Deliver insulin for treatment
Receive insulin injection
<<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-03: Administer insulin only according to validated infusion parameters and prevent unauthorized dosages [SC-01]
<<safetyGoal>>
R-04: Monitor timing and quantity of delivery to ensure correct dose is given at the right time [SC-02]
<<safetyGoal>>
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
Take insulin measurements
Take blood measurements
<<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-08: Respond physiologically to insulin in a way that is consistent with treatment expectations (acknowledging variability) [SC-02]
Receive insulin infusion
E3 - Infusion set
Administer insulin
Administer insulin injection
<<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-06: Maintain physical integrity to prevent leaks or unintended flow of insulin [SC-01]
<<safetyGoal>>
R-07: Ensure correct and timely delivery of insulin from pump to patient [SC-02]

Step 3 - Define the Control Structure



Step 4 - Identify Unsafe Control Actions (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	**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	*Not applicable*

			prescribed, leading to underdose [H1]	administration and resulting in hypoglycemia [H2]	

Additional hazards cause identified independently of the STPA results

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

Step 5 - Identify 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.

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)*
UCA-02: Patient provides “Program insulin dosage” with a value higher than prescribed, leading to overdose [H2]	**LS-03:** The patient repeats a bolus due to lack of feedback on recent insulin administration. [UCA-02] *Zhang et al. (2010)* **LS-04:** Patient misinterprets the prescribed dose and enters a value higher than medically indicated. [UCA-02] *Zhang et al. (2011)*	**SR-03:** The system shall display recent insulin activity clearly before accepting a new dose. [LS-03] *Zhang et al. (2011)* **SR-04:** The system shall cross-check manual input with prescription data and alert if excess dosage is detected. [LS-04] *Zhang et al. (2011)*
UCA-03: Patient provides “Program insulin dosage” with a value lower than prescribed, leading to underdose [H1]	**LS-05:** The patient reduces the dose to avoid hypoglycemia without clinical basis. [UCA-03] *Martinazzo (2022)* **LS-06:** The system does not notify that the entered dose is below clinical expectation. [UCA-03] *Zhang et al. (2011)*	**SR-05:** The system must recommend confirmation when the user’s dose is significantly below the recommended amount. [LS-05, LS-06] *Zhang et al. (2011)*
UCA-04: Patient provides “Program insulin dosage” too late, leading to hyperglycemia [H1]	**LS-07:** The patient delays programming due to being busy or distracted, compromising glycemic control. [UCA-04] *Martinazzo (2022)* **LS-08:** The system accepts bolus entry even after blood glucose spike already occurred. [UCA-04] *Ribeiro et al. (2024)*	**SR-06:** The interface must issue periodic prompts for pending bolus if blood glucose remains elevated and no dose is scheduled. [LS-07] *Zhang et al. (2011)* **SR-07:** The system must block bolus entries considered ineffective post-prandial, requiring physician override. [LS-08] *Ribeiro et al. (2024)*

UCA-05: Patient provides “Program insulin dosage” too early, leading to premature insulin administration and resulting in hypoglycemia [H2]	**LS-09:** Patient programs insulin and forgets to eat, leading to insulin drop without carbohydrate intake. [UCA-05] *Zhang et al. (2010)* **LS-10:** Patient assumes a meal is imminent, but it is delayed due to unforeseen events. [UCA-05] *Martins et al. (2015)*	**SR-08:** System must require user confirmation that the meal is occurring before completing bolus delivery. [LS-09] *Zhang et al. (2011)* **SR-09:** If a meal confirmation is not received within a set time, bolus must be suspended or canceled automatically. [LS-10] *Martins et al. (2015)*

Additional hazards cause identified independently of the STPA results

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.

Step 7 - Update the iStar4Safety Models