Automated Insulin Delivery (AID) System
STPA-SafeSecIoT Analysis – Steps 1 and 2

Step 1. Define the purpose of the analysis

Defining Losses (L)

- L1: Loss of life or life-threatening to the patient (acute incident of hypo/hyperglicemia, diabetic coma, and others);
- L2: Loss of or damage to the AID system components;
- L3: Loss of mission (automated insulin delivery);
- L4: Loss of or corruption of sensitive information;
- L5: Loss of connectivity between components of the system.

Defining System-level Hazards (H) and Threats (T)

- H1: The BG sensor is unable to read BG data [L1, L3];
- H2: The CGM is unable to send BG readings to the control application [L1, L3, L4, L5];
- H3: The CGM physical integrity is lost [L1, L2, L3]; % with compromised physical integrity
- H4: The control application cannot calculate or incorrectly calculates the insulin dose to place the BG into a target range [L1, L3];
- H5: The control application cannot calculate or incorrectly calculates the insulin dose for meal-correction bolus [L1, L3];
- H6: The control application cannot track or incorrectly tracks residual insulin [L1, L3];
- H7: The control application does not provide an alarm for hypo/hyperglycemia limits [L1, L3, L4];
- H8: The control application is unable to receive readings from the CGM [L1, L3, L4, L5];
- H9: The control application is unable to send instructions to the IP [L1, L3, L4, L5];

- H10: The patient does not provide meal data to calculate the meal-correction bolus [L1, L3];
- H11: The IP delivers the wrong dose to the patient in either amount or timing [L1, L3];
- H12: The IP with compromised physical integrity [L1, L2, L3];
- H13: The IP is unable to pair and receive data to the control application [L1, L3, L4, L5];
- H14: The IP reservoir volume is not monitored [L1, L2, L3].

- T1: Communications between components transmitted in clear text [L1, L3, L4, L5];
- T2: Weak pairing protocol between components [L1, L3, L4, L5];
- T3: Lack of mechanisms to prevent replay attacks or guarantee transmission [L1, L3, L4, L5].

Step 2. Model the control structure

Defining Responsabilities (R) and associate components

- R1: Perform blood glucose measurement (CGM);
- R2: Check/calculate the need for basal insulin (App);
- R3: Check/calculate the need for insulin for meal correction bolus (App);
- R4: Deliver (apply) insulin (IP).

Defining Control Actions (CA)

- CA1: Measure blood glucose;
- CA2: Release basal insulin;
- CA3: Release meal correction bolus;
- CA4: Deliver (apply) insulin.

Functional Control Structure