Safety Analysis of a Low-cost Insulin Infusion Pump using STPA: A Case Study with a Brazilian Company

2021 MIT STAMP Workshop

Aldo Martinazzo martinazzoaldo@gmail.com

Luiz Eduardo Galvão Martins martinsleg@hotmail.com

Sebastião Vagner Aredes vagner@deltalife.com

Tatiana Sousa Cunha ts.cunha@unifesp.br

Type 1 Diabetes Mellitus

Type 1 Diabetes Mellitus

- Disease that affects the metabolism of nutrients
- Caused by lack of insulin production by pancreas

Type 1 Diabetes not adequately treated causes:

- Acute crises of hyperglycemia: blood glucose too high, and
- Long- term complications

Cardiovascular diseases

Kidney disease

Diabetic eye disease

Amputation of lower limbs

Source: International Diabetes Federation (IDF), "IDF Diabetes Atlas" 9th ed. 2019

Therapy for Type 1 Diabetes Mellitus

Intensive insulin therapy for type 1 diabetes

- Protects against complications
- Introduces the risk of hypoglycemia: blood glucose too low
  - Both hyperglycemia and hypoglycemia can be life threatening

Continuous subcutaneous insulin infusion (CSII)

Insulin infusion pump

Multiple Daily Injections (MDI)

Insulin pen

Sources:
https://www.flaticon.com/free-icon/insulin_3003865 https://www.flaticon.com/free-icon/insulin_3113755

Insulin Pump Therapy versus Multiple Daily Injections

Insulin pump therapy compared with MDI:

- Provides better blood glucose control, and
- allows a less restricted lifestyle to patient
- However, its cost is higher
  - There is no insulin infusion pump manufactured in Brazil
  - The imported ones are expensive, which limits their use

- Development of a more affordable insulin infusion pump:
  - Federal University of São Paulo
  - *DeltaLife*, a Brazilian company of medical equipment

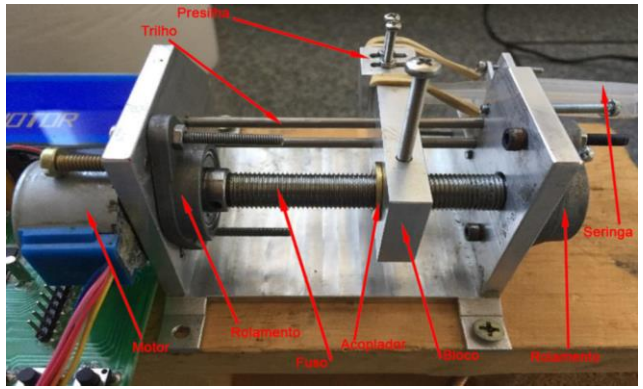
Development team

Multidisciplinary team, including:

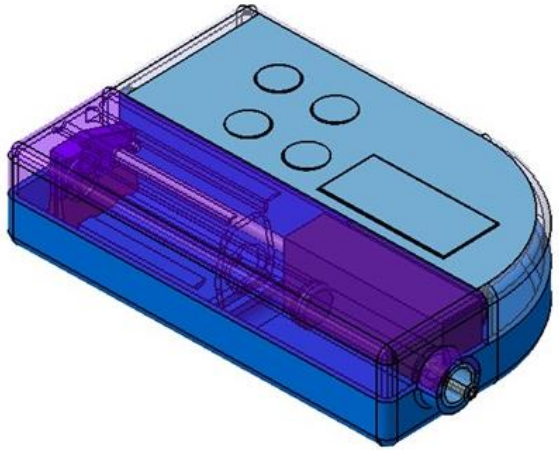
- Researchers from the Federal University of São Paulo:
  - Health care for diabetic people,
  - Software development,
  - Electronic design,
  - Mechanical design,
  - Risk Management
- Chief Engineer of *DeltaLife*

Development evolution

Proof of concept



Present prototype

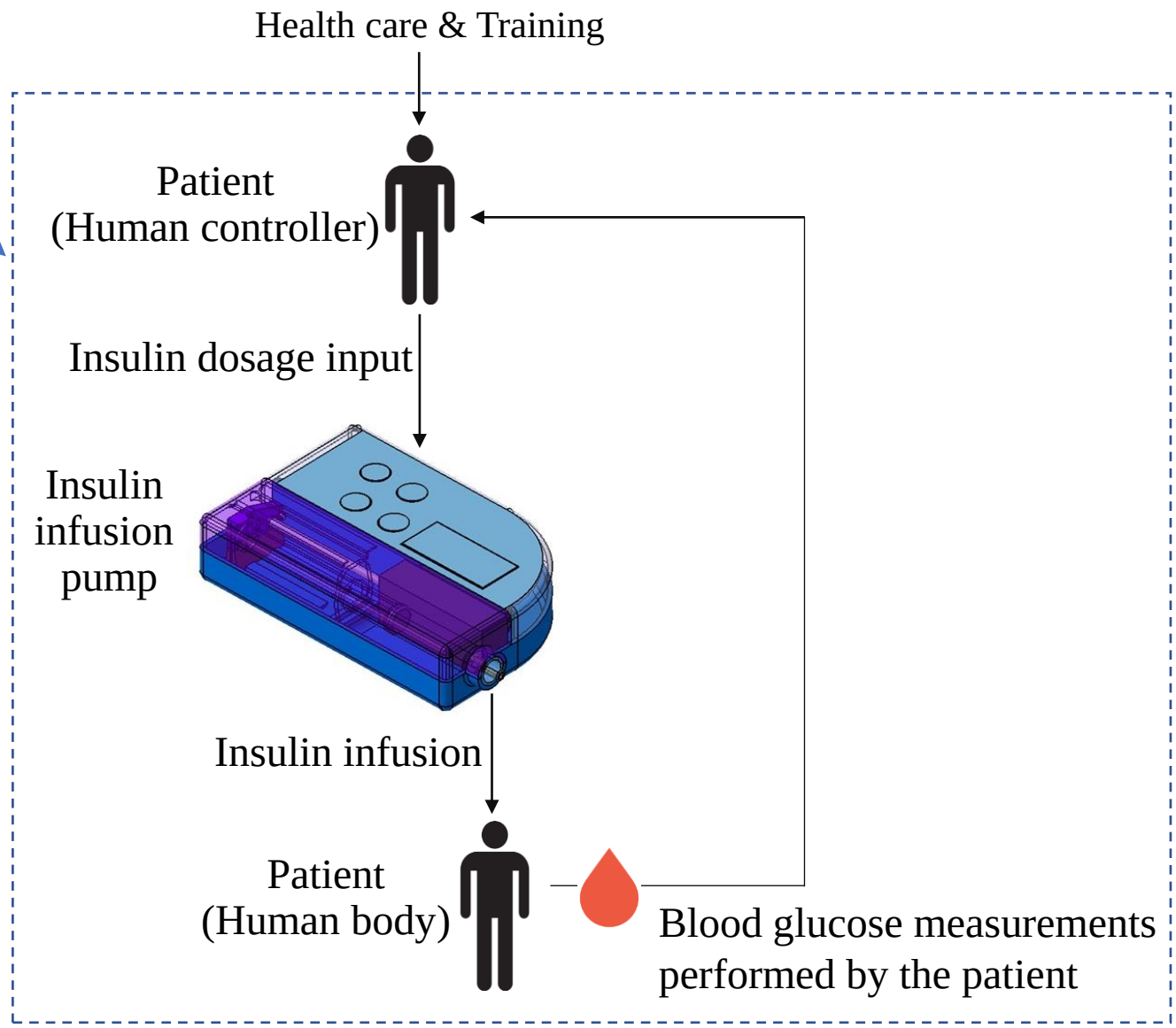


Purpose of the safety analysis using STPA: to support the insulin pump architectural design from a safety perspective.

Insulin pump therapy

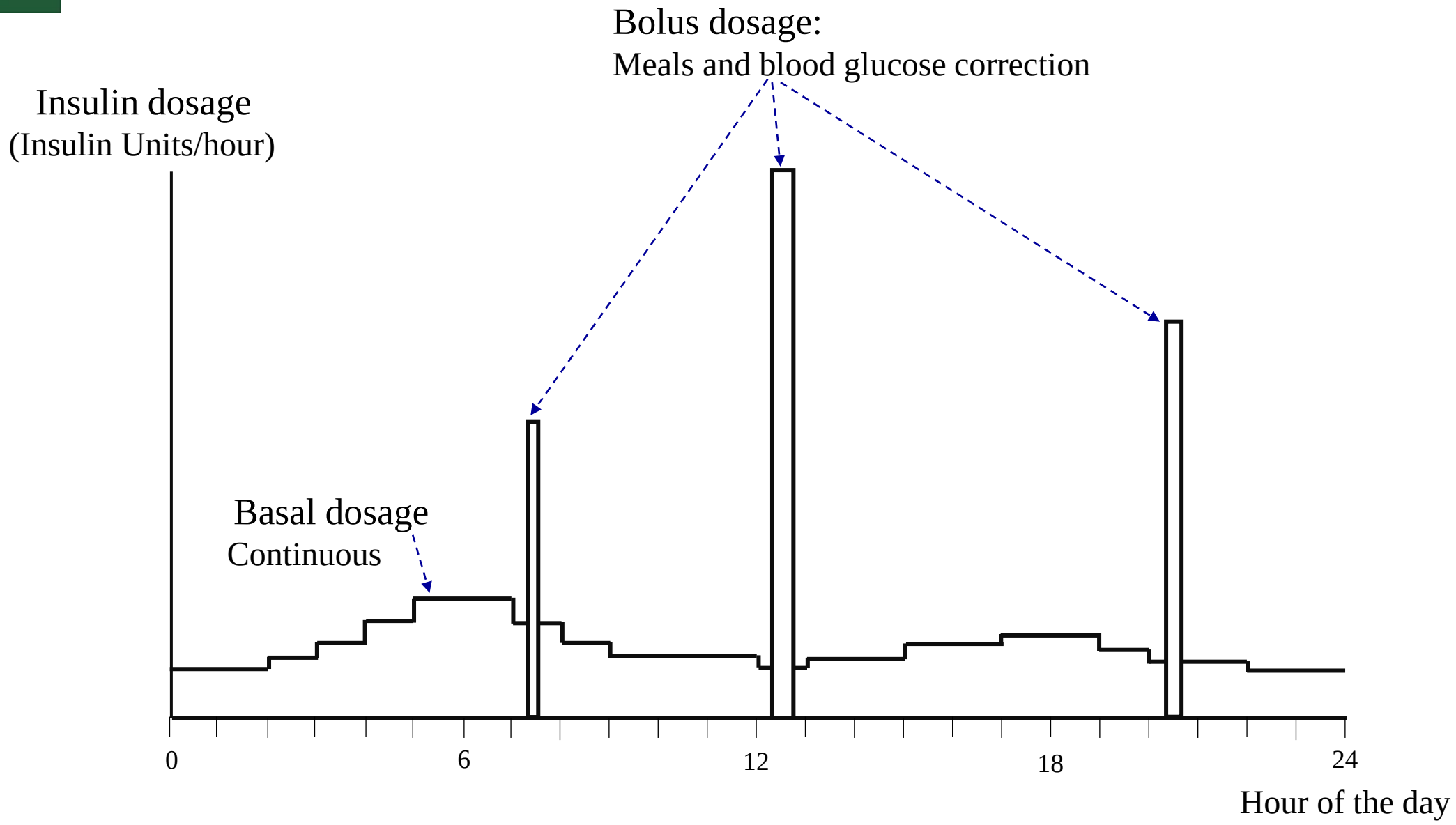
System under analysis

Intensive insulin therapy for type 1 diabetes, with insulin infusion pump



Insulin dosage

- Insulin pump therapy



Loss and System Level Hazards

Loss to be prevented:

L-1: Patient death or life-threatening injury

System level hazards:

H1: Hypoglycemia, with blood glucose below 54 mg/dL

- Mental confusion
- Visual disturbances
- Coma

H2: Hyperglycemia, with blood glucose above 250 mg/dL

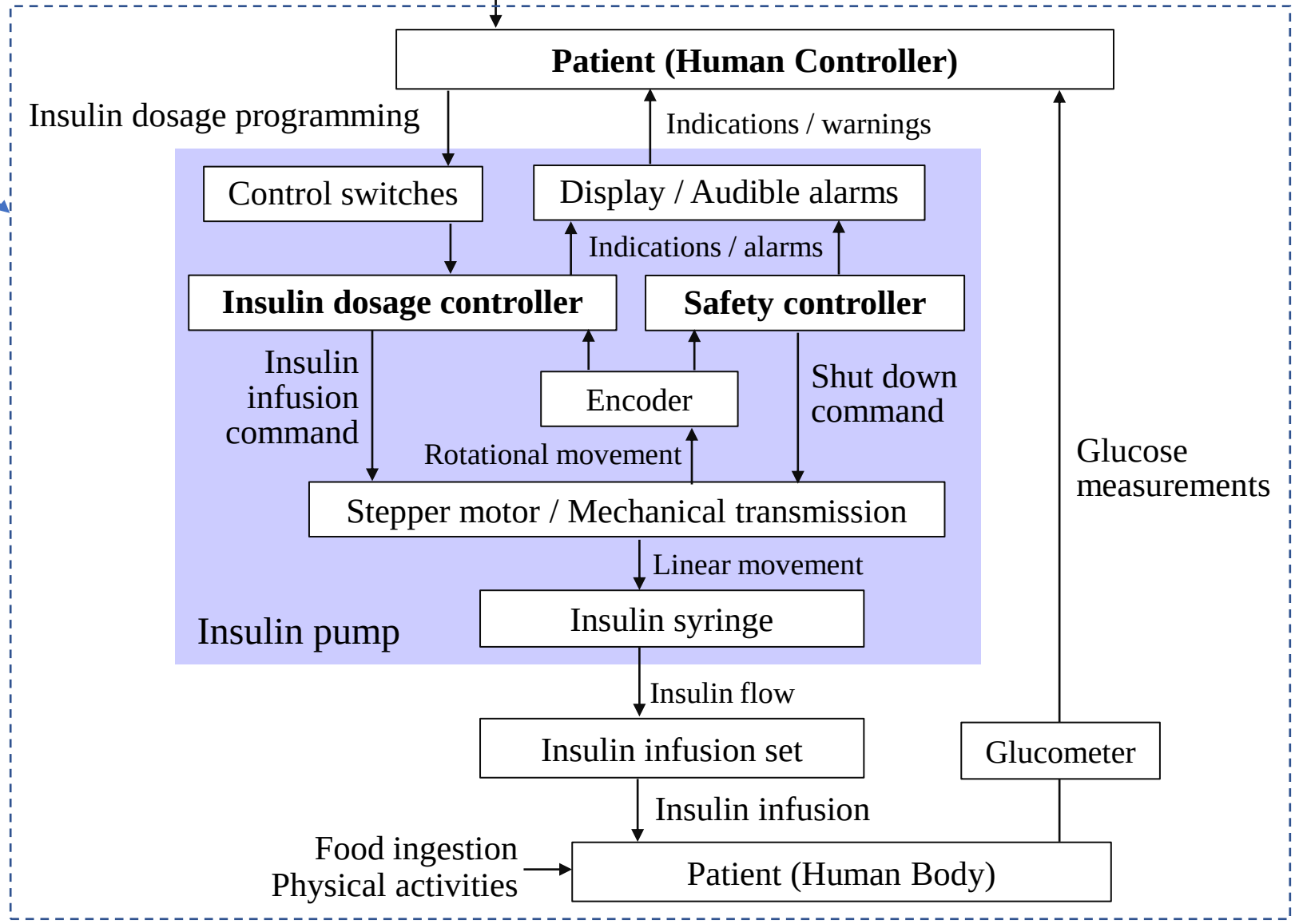
- Ketoacidosis: increased blood acidity
- Confusion
- Coma

Hierarchical Control Structure Model

Health care: Diabetes / complications
Training: Glucose management / insulin pump operation

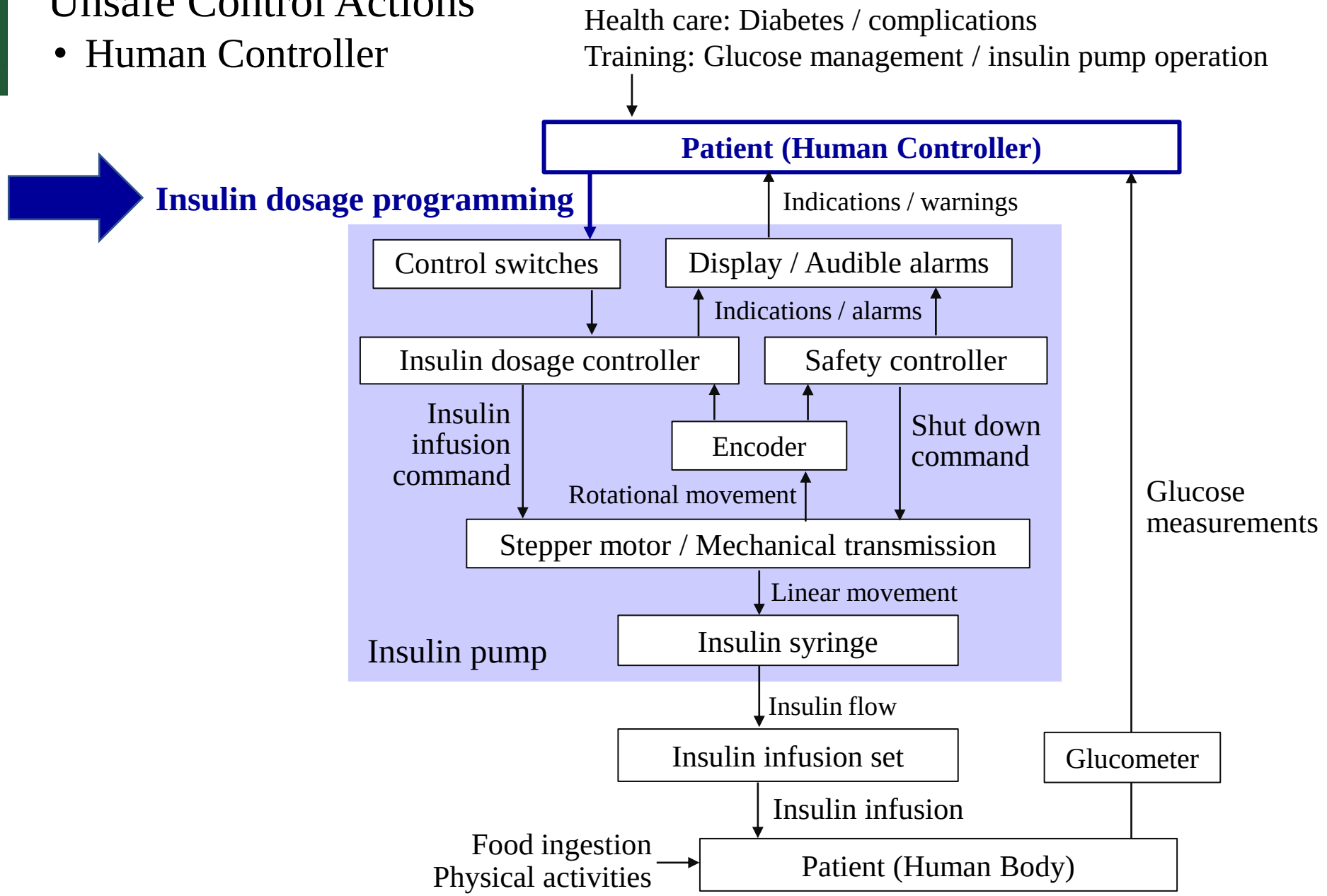
System boundary

Improved the interaction with heterogeneous specialties



Unsafe Control Actions

- Human Controller



Unsafe Control Actions

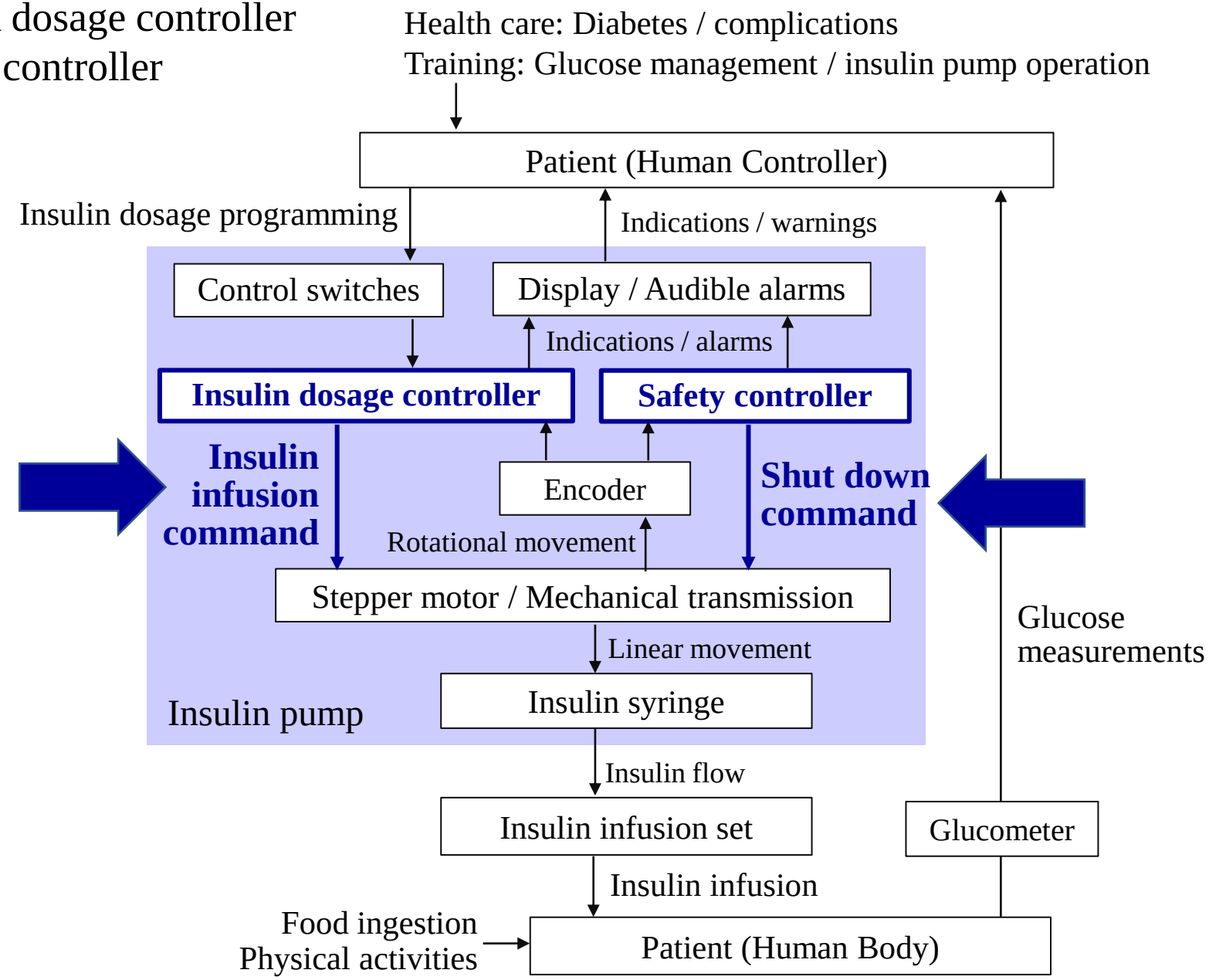
- Human Controller

Unsafe control Actions of Human Controller

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Program insulin dosage	Human controller does not program bolus for meal or blood glucose correction Human controller does not adjust basal dosage for physical activities.	Human controller programs excessive bolus dosage Human controller programs insufficient bolus dosage Human controller programs excessive basal dosage Human controller programs insufficient basal dosage Human controller interrupts infusion inadvertently.	Human controller programs bolus too late in response to meal Human controller programs basal dosage for each hour of the day out of order	Human controller programs bolus too long Human controller programs bolus too short

Unsafe Control Actions:

- Insulin dosage controller
- Safety controller



Unsafe Control Actions:

- Insulin dosage controller
- Safety controller

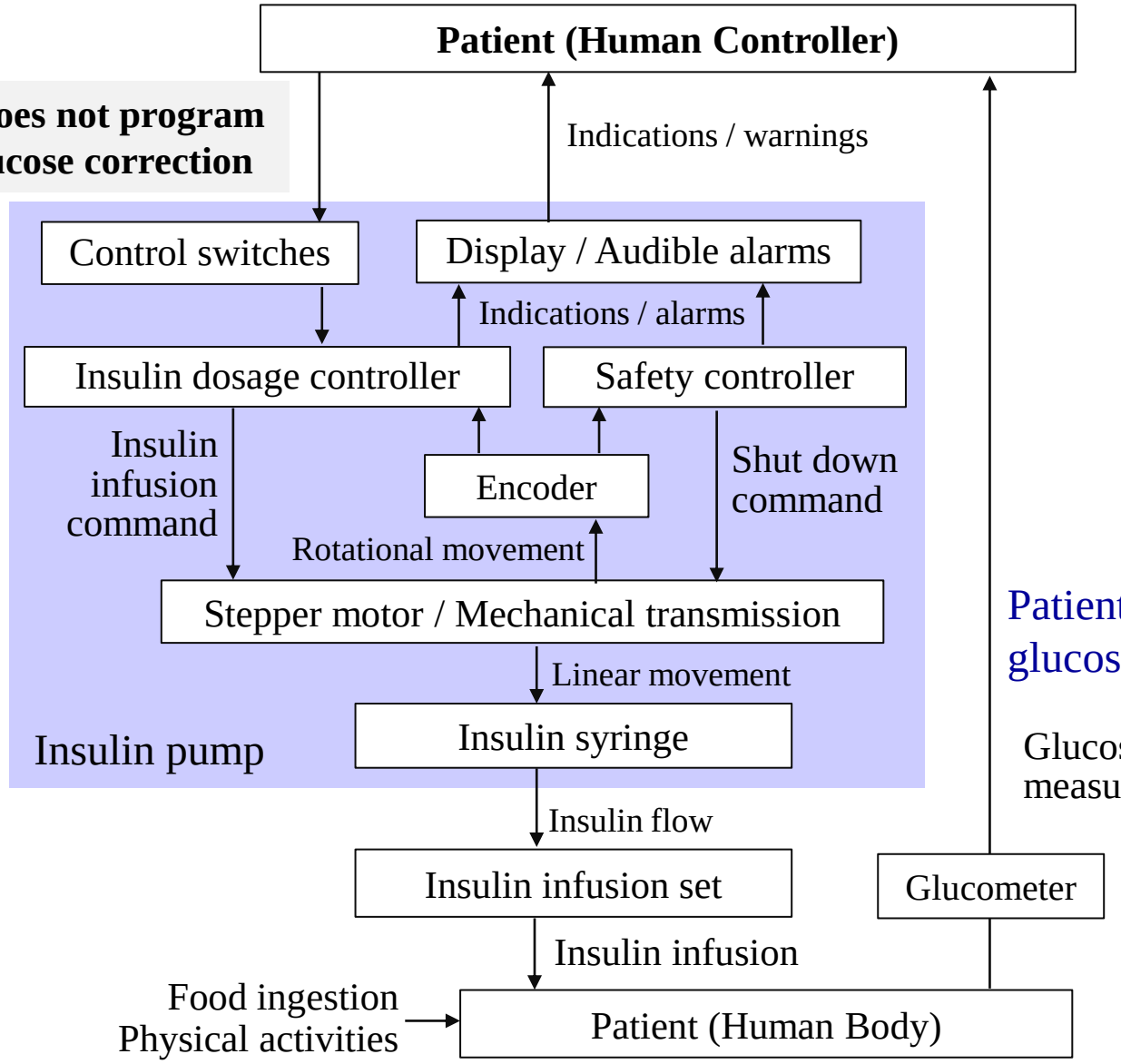
Unsafe control Actions of Insulin Dosage Controller and Safety Controller

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Insulin infusion command	Dosage controller does not provide command for basal insulin Dosage controller does not provide command for bolus Dosage controller does not provide command for basal and bolus	Dosage controller commands excessive basal insulin Dosage controller commands insufficient basal insulin Dosage controller commands excessive insulin bolus Dosage controller commands insufficient insulin bolus Dosage controller commands excessive insulin infusion	Dosage controller commands basal insulin for each hour of the day out of order	Dosage controller commands insulin bolus too long Dosage controller commands insulin bolus too short
Automatic shut down	Safety controller does not shut down stepper motor in case of over-infusion	Safety controller shuts down stepper motor when not required, leading to infusion interruption	Safety controller shuts down stepper motor too late in case of over-infusion	

Loss scenarios for UCA of Human Controller

UCA: Human controller does not program bolus for meal or blood glucose correction

Patient ingests food but does not program corresponding bolus



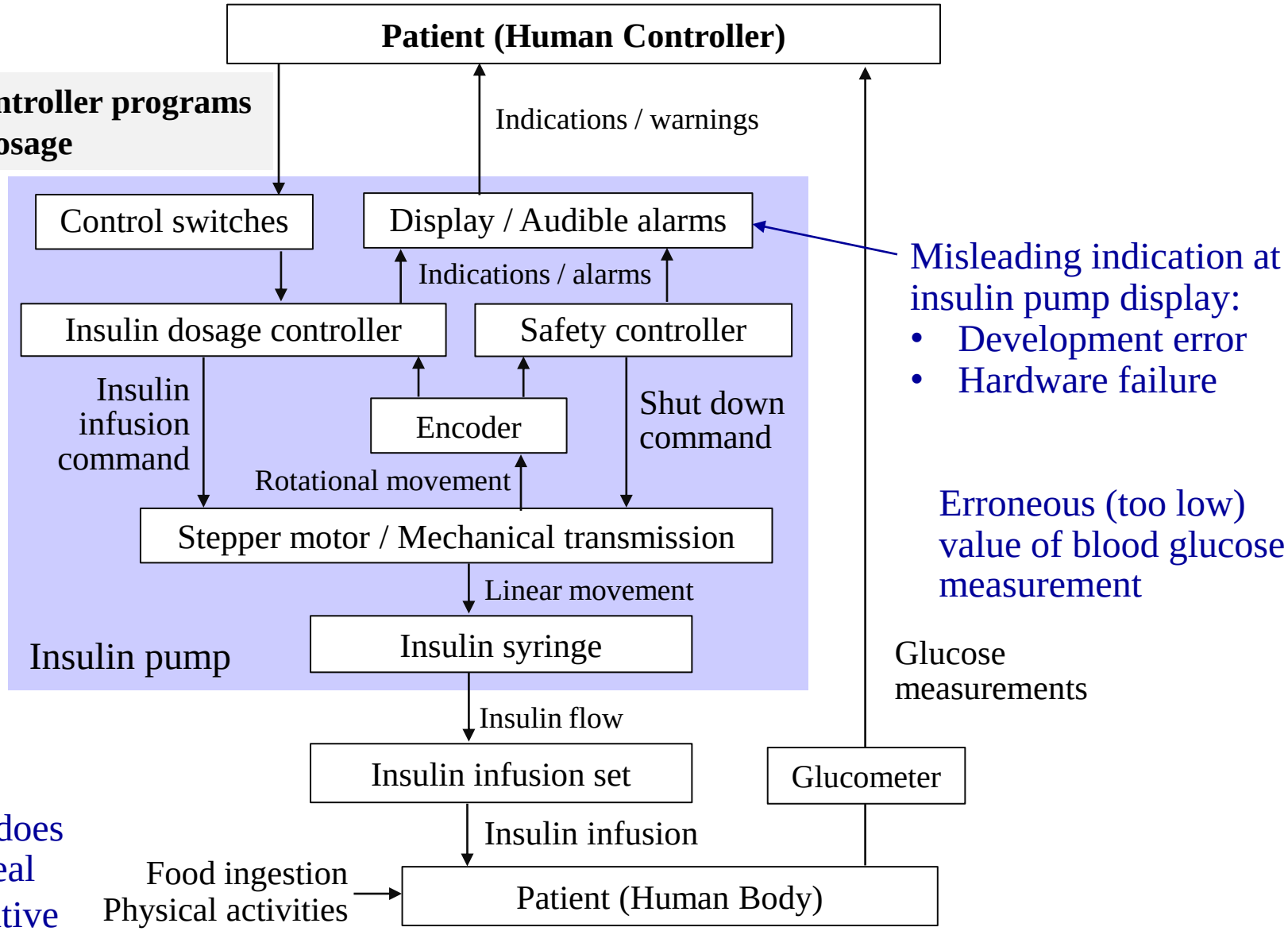
Patient does not perform blood glucose measurement

Glucose measurements

Loss scenarios for UCA of Human Controller

UCA: Human controller programs excessive bolus dosage

Erroneous programming of insulin pump by patient



Misleading indication at insulin pump display:

- Development error
- Hardware failure

Erroneous (too low) value of blood glucose measurement

- Patient programs bolus but does not ingest corresponding meal
- Erroneous (too high) estimative of meal carbohydrate

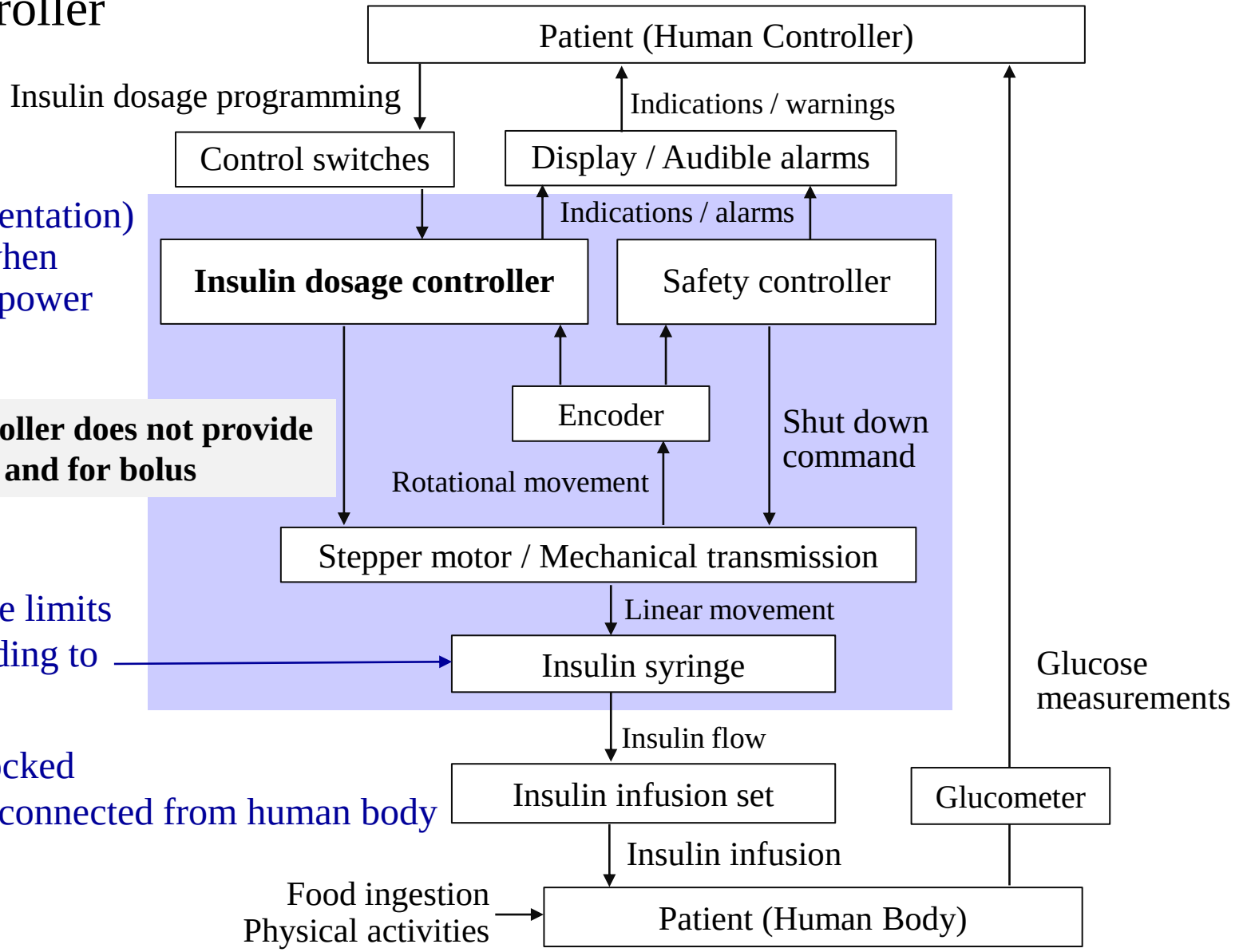
Loss scenarios for UCA of Insulin dosage controller

- Software flaw (requirement / implementation)
- Patient does not replace the battery when required, leading to loss of electrical power
- Physical components failure

UCA: Dosage controller does not provide command for basal and for bolus

- Insulin pump used out of temperature limits
- Patient does not replace syringe, leading to lack of insulin.

- Infusion set blocked
- Infusion set disconnected from human body

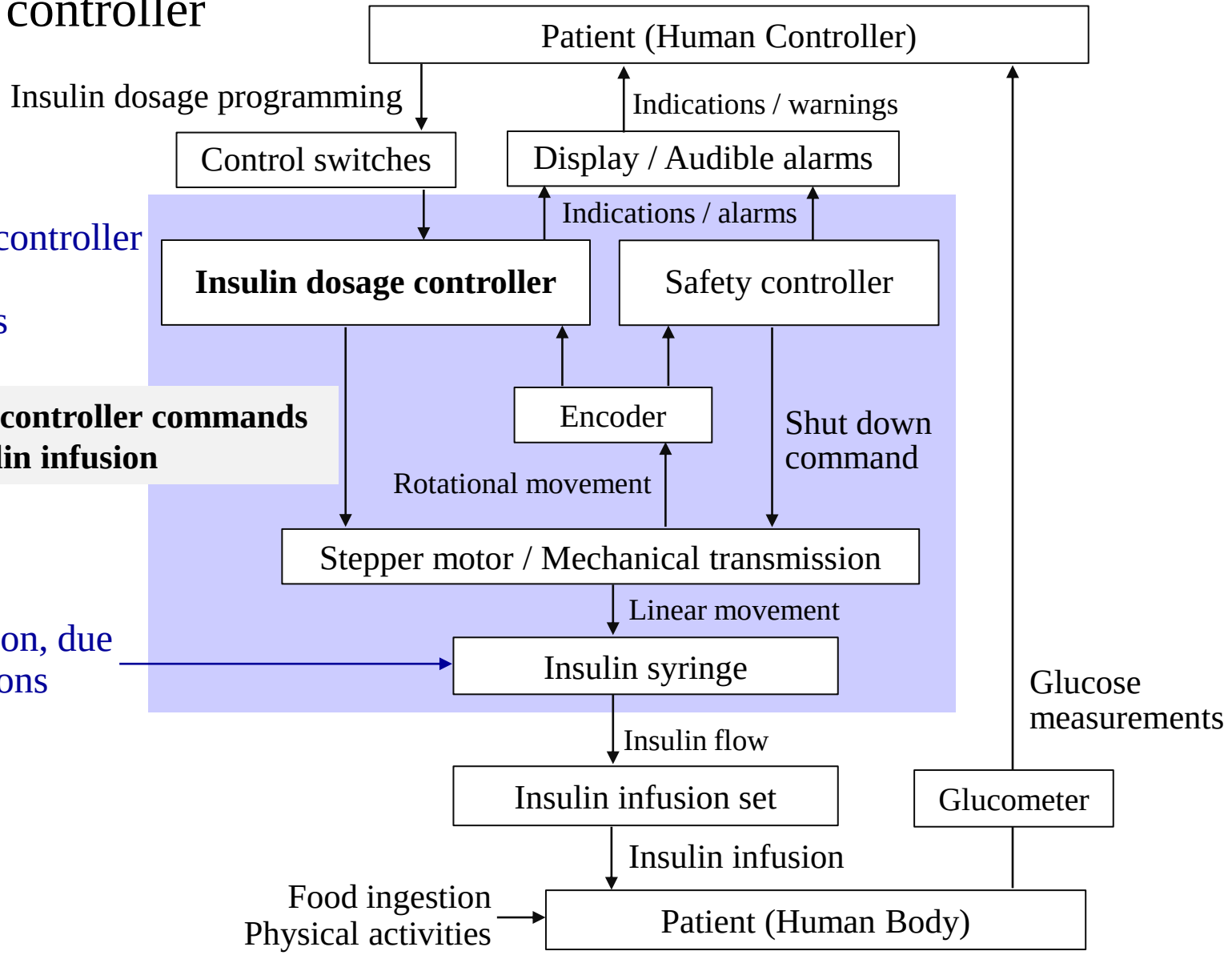


Loss scenarios for UCA of Insulin dosage controller

Erroneous command of dosage controller
- Software flaw
- Electromagnetic disturbances

UCA: Dosage controller commands excessive insulin infusion

Unintended syringe actuation, due to ambient pressure variations



Requirements from STPA analysis

- Support insulin pump architectural design from the safety point of view

Examples of safety requirements arising from STPA analysis

Unsafe Control Action	Loss scenario	Requirements to prevent loss scenarios
Human controller programs excessive bolus dosage	Patient performs erroneous (too high) estimative of meal carbohydrate Patient performs erroneous (too low) blood glucose measurement	Selection criteria for insulin pump user: • Proficiency on carbohydrate estimative and blood glucose measurement
	Human controller erroneous programming of the insulin pump	Proficiency on insulin pump use: • User manual • Training Insulin pump user interface design: • User friendly • Limit for maximum and minimum dosage input
Dosage controller commands excessive insulin infusion	Unintended syringe actuation, due to ambient pressure variations	Syringe plunger shall not move due to ambient pressure variations within the operational environment.

Acknowledgments:

- Ana Lucia Neves
- Fernanda Tenório
- Marcia Reberte
- Ricardo Kenji

Thanks for the attention!!!

Questions?

Aldo Martinazzo martinazzoaldo@gmail.com

Luiz Eduardo Galvão Martins martinsleg@hotmail.com

Sebastião Vagner Aredes vagner@deltalife.com

Tatiana Sousa Cunha ts.cunha@unifesp.br

Bibliographic references

- Leveson NG, Thomas JP, STPA Handbook, 2018
- International Diabetes Federation (IDF), IDF Diabetes Atlas, 9th ed.2019
- Nathan DM, The diabetes control and complications trial/epidemiology diabetes interventions and complications study at 30 years: overview. Diabetes Care, 2014, v. 37, n.1, p. 9-16.
- Martins LEG, Faria H, Vecchete L, Cunha T, Oliveira T, Casarini DE, et al. Development of a Low-Cost Insulin Infusion Pump: Lessons Learned from an Industry Case. In: 2015 IEEE 28th International Symposium on Computer-Based Medical Systems. IEEE. 2015, p. 338–343
- Tenório FS, Martins LEG, Cunha TS, Accuracy of a low-cost continuous subcutaneous insulin infusion pump prototype: in vitro study using combined methodologies, Annals of Biomedical Engineering, 2021.
- Golberg A, Vasques ACJ, Faria ACRA, Lottenberg AMP, Joaquim AG, Vianna AGD, et al. Diretrizes Sociedade Brasileira de Diabetes 2019-2020. Clannad, 2019
- Gabbay MAL, Manual prático de bombas de insulina, Clannad, 2019