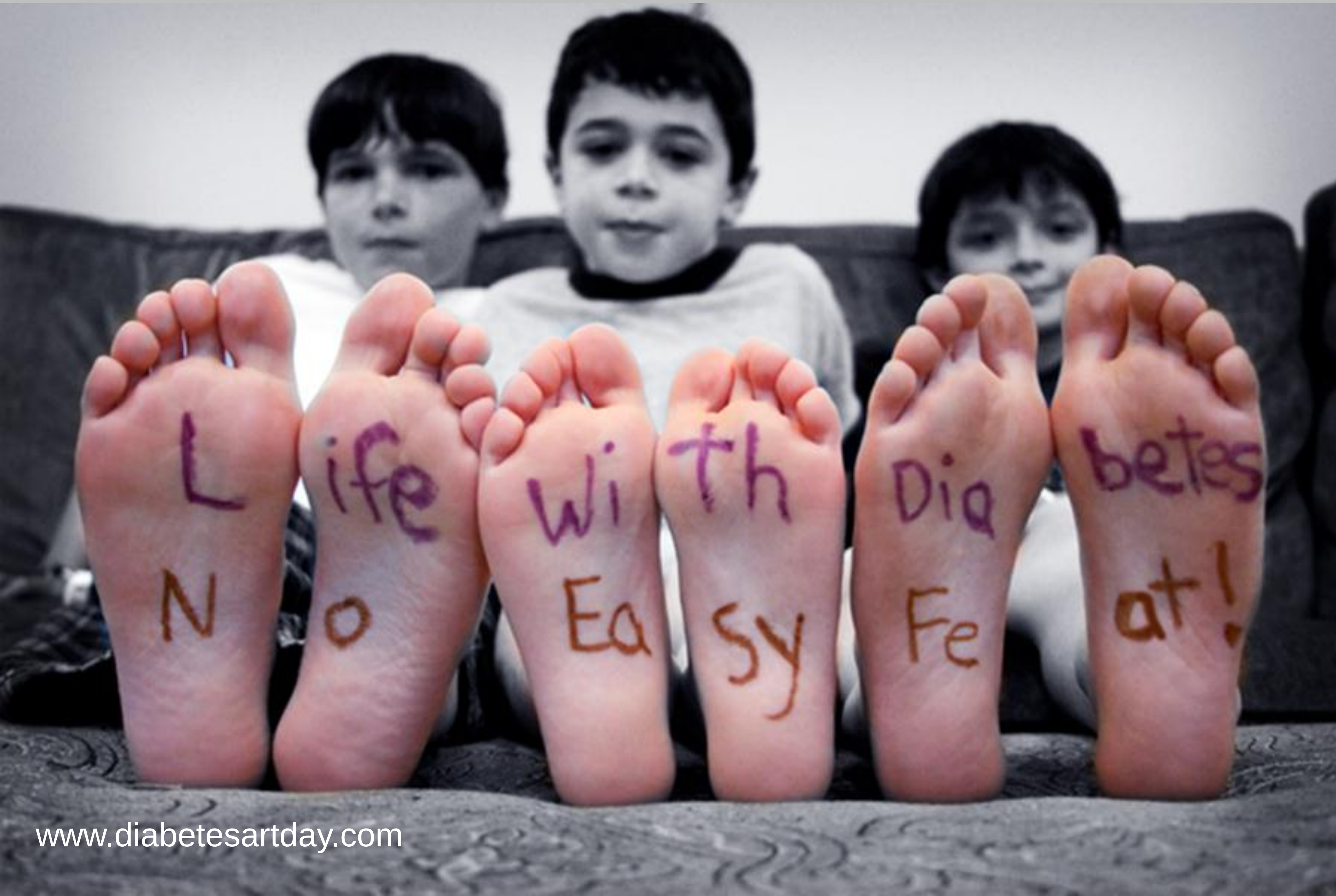
Applying STPA to the Artificial Pancreas for People with Type 1 Diabetes

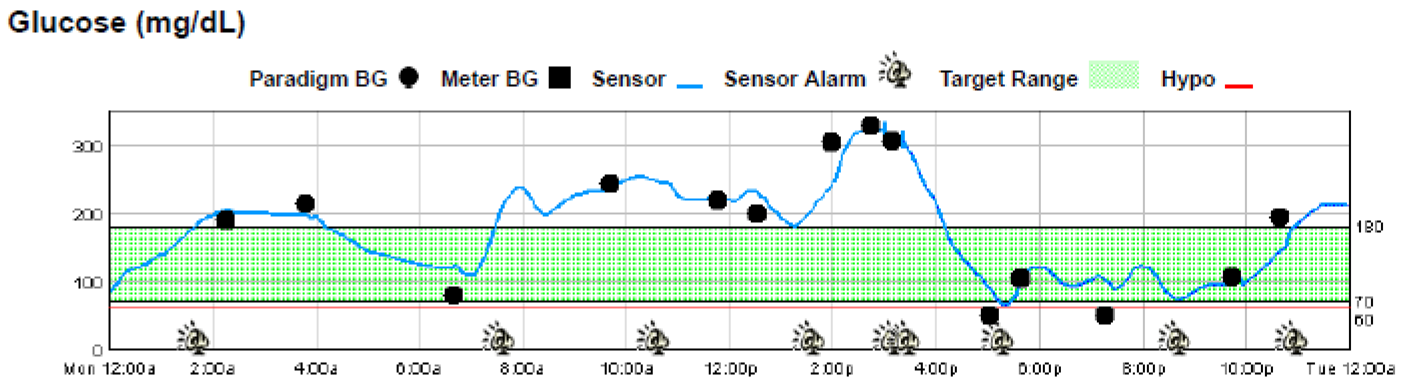
Lane Desborough
Product Strategist
Medtronic Diabetes
Northridge, California

- **Type 1 Diabetes**
- Artificial Pancreas
- Challenges
- Applying STPA

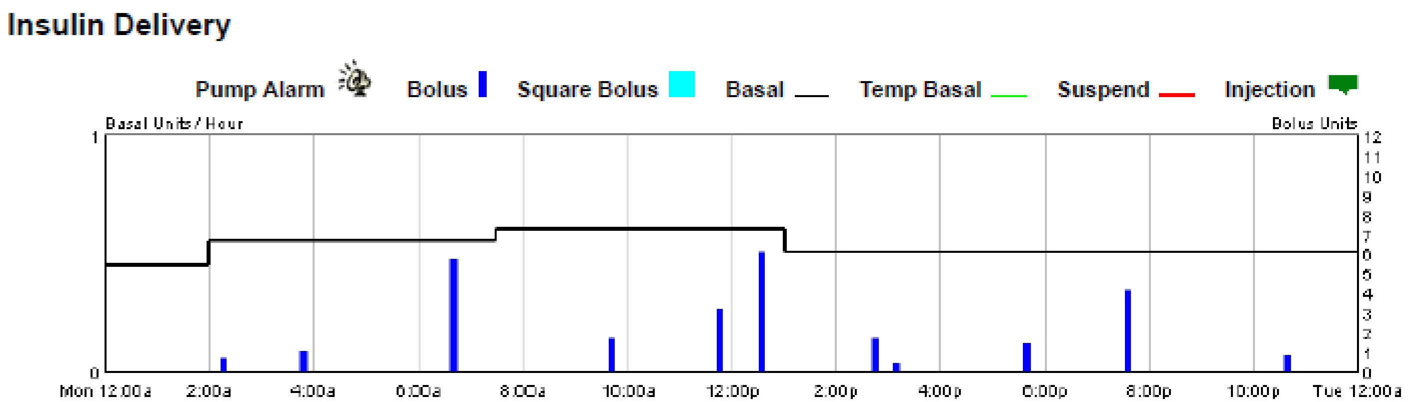
Type 1 Diabetes is a Huge Burden



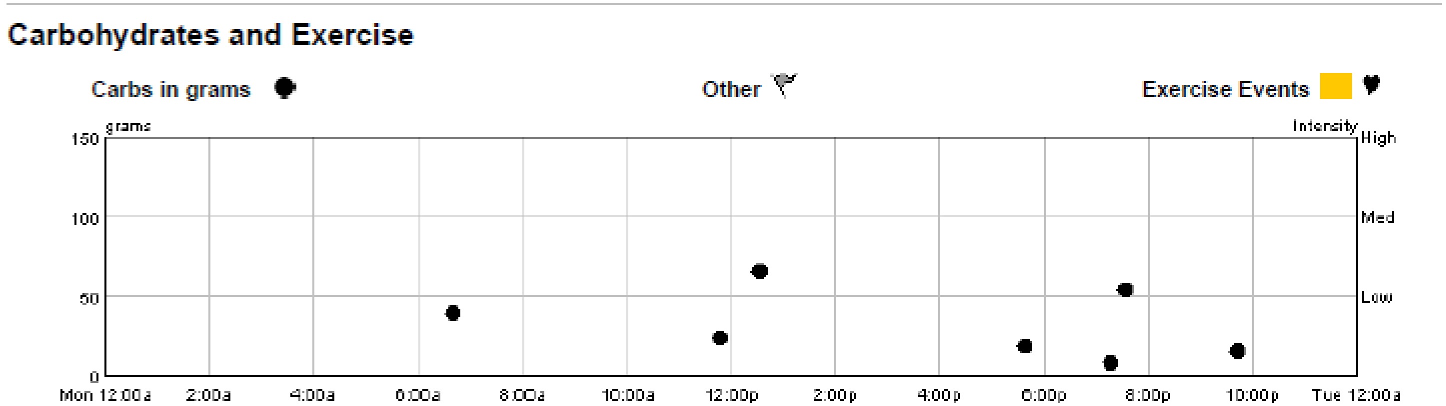
Blood Glucose



Insulin



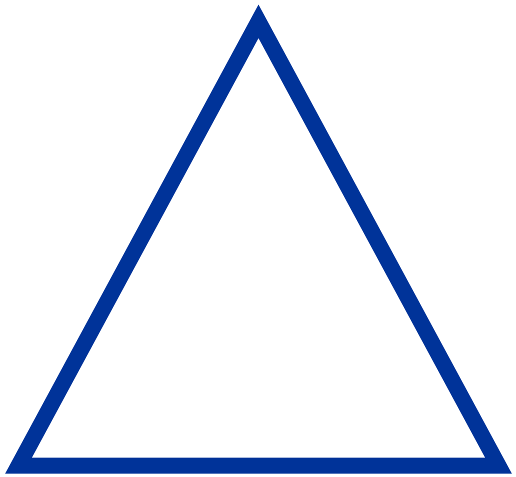
Food and Exercise



Control / Effort / Flexibility: Pick up to Two

Glucose Control

- Acute dangers
- Chronic complications



Lifestyle Flexibility

- Food, exercise, sleep
- Time, type, place, amount

Therapy Effort

- Carb counting, pre-meal bolusing
- Bolus / basal adjustment
- Therapy compliance
- Experimentation, problem solving, collaboration, learning

Medtronic

Living with Diabetes: Hayden Desborough

http://www.youtube.com/watch?v=478Vr81rws0&feature=player_embedded

- Type 1 Diabetes
- **Artificial Pancreas**
- Challenges
- Applying STPA

Artificial Pancreas

algorithm

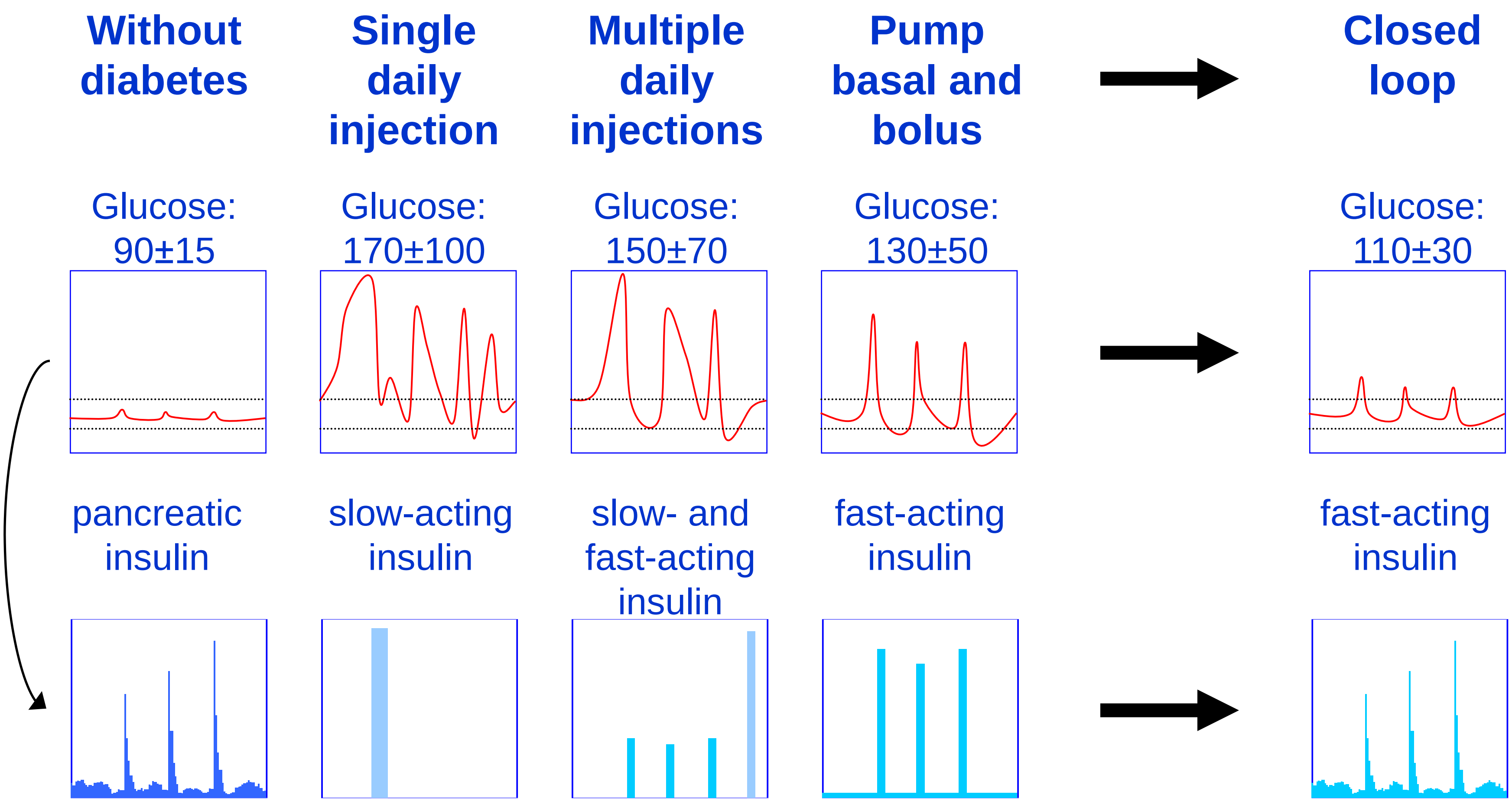
Sense

Decide

Act

Medtronic

Artificial Pancreas: safely transfer variation from blood glucose to insulin in order to make living with diabetes easier

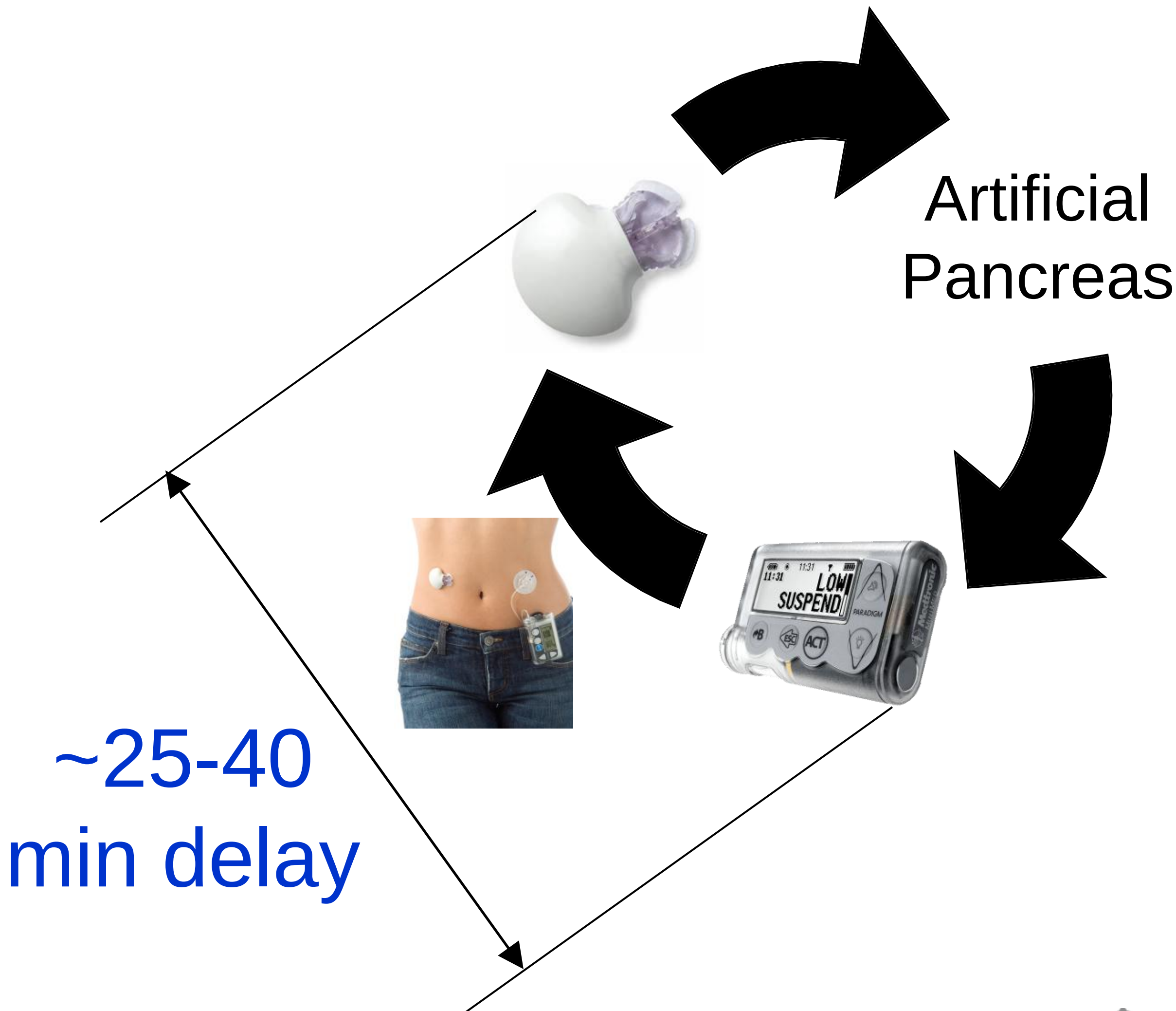


- Type 1 Diabetes
- Artificial Pancreas
- **Challenges**
- Applying STPA

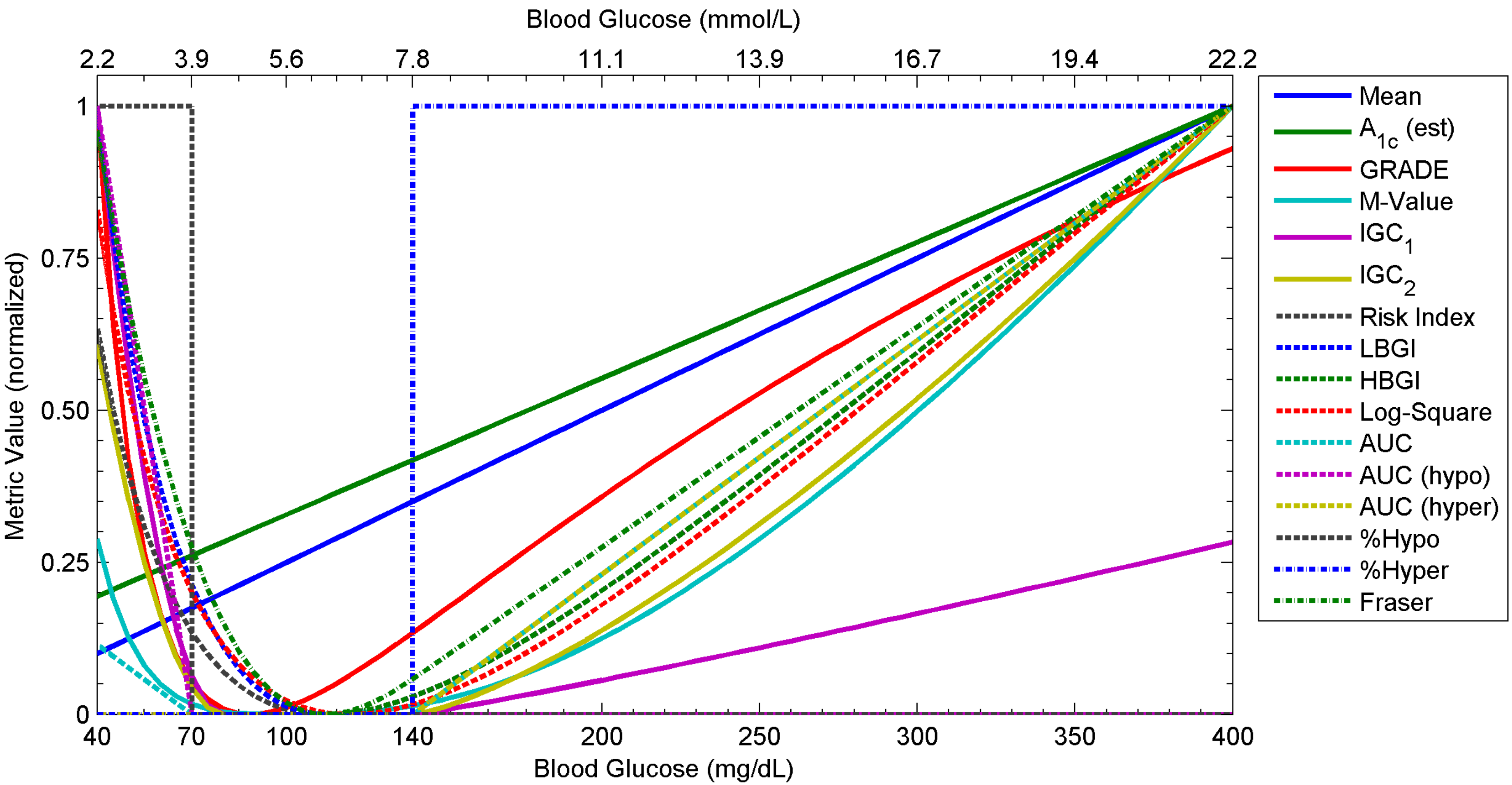
1. There are many *sources* of variation

Timing	Events
Every 3-7 years	1. Complications 2. Physiological changes
Every year	3. Serious events 4. Illness stress
Every quarter	5. Travel / time zone changes 6. Psychological stress
Every week	7. Missed meals 8. Restaurant meals
Every 3 days	9. Hormonal stress 10. Psychological stress
Every meal	11. Circadian rhythms 12. Exercise stress
Every hour	13. Normal meals
Every minute	14. Movement

2. There is a limit to how much variation *can* be transferred



3. There isn't consensus on ***which*** variation to transfer (which loss function to use)



Medtronic

4. There is a limit to how much variation *should* be transferred

"Blink"

Humans are good at:

"Recognition"

- Pattern recognition
- Troubleshooting
- New situations

"Think"

Computers are good at:

"Cognition"

- Vigilance / repetitive tasks
- Fast response to defined situations
- Automated procedures

Improper task allocation between the human and the artificial pancreas may result in:

- High cognitive load from supervisory task
- Automation-induced complacency
- Brittleness (opposite of resiliency)
- Mistrust of automation
- Erosion of expertise and engagement

Medtronic

5. There are challenges in Sensing, Deciding, and Acting

Sense: My actual blood glucose…may not be what I'm sensing

Sensor Site → Sensor → Transmitter → Calibration → Sensor Value

- **Sensor Site:** Compressed, Fatigued, Slow Dynamics
- **Sensor:** Pulled out, Old, Noisy, Disconnected, Drifting, Biased, Non-linear
- **Transmitter:** Dead battery, Wireless blocked, Wireless spoofed
- **Calibration:** Outdated strips, Contaminated fingers, Missed
- **Sensor Value:** Inaccurate, Missing, Deadtime, Lag, Dead battery,

Decide: The right amount of insulin … may be unknown

External disturbances (meals, exercise, stress, illness) – future or unmeasured

Physiological variations (hourly / daily / monthly / yearly) – changing or unmeasured

Act: The insulin dose I want… may not be what I get

Insulin → Pump → Infusion Set → Infusion Site

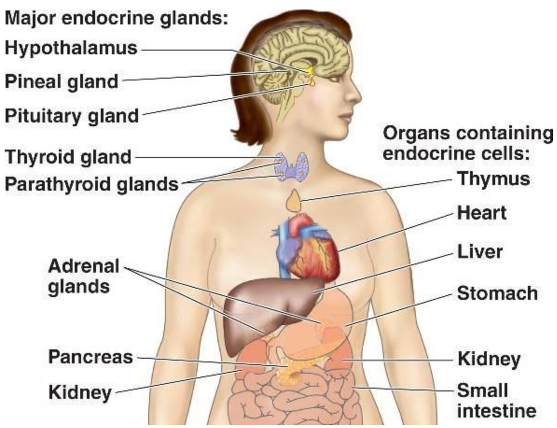
- **Insulin:** Wrong kind, Slow acting, Degraded (old, fried), Air entrained
- **Pump:** Wrong bolus type, Wrong bolus amount, Dead battery
- **Infusion Set:** Occlusion, Cold, Disconnected, Air-in-line
- **Infusion Site:** Compressed, Fatigued, Intramuscular, intravenous, Pulled-out, Slow Dynamics

Medtronic

6. Great care must be taken when introducing feedback into hazardous software-intensive sociotechnical systems

Hazards + Humans + Software + **Feedback**

7. It's hard to control a multi-input, multi-output system with a single-input, single-output controller



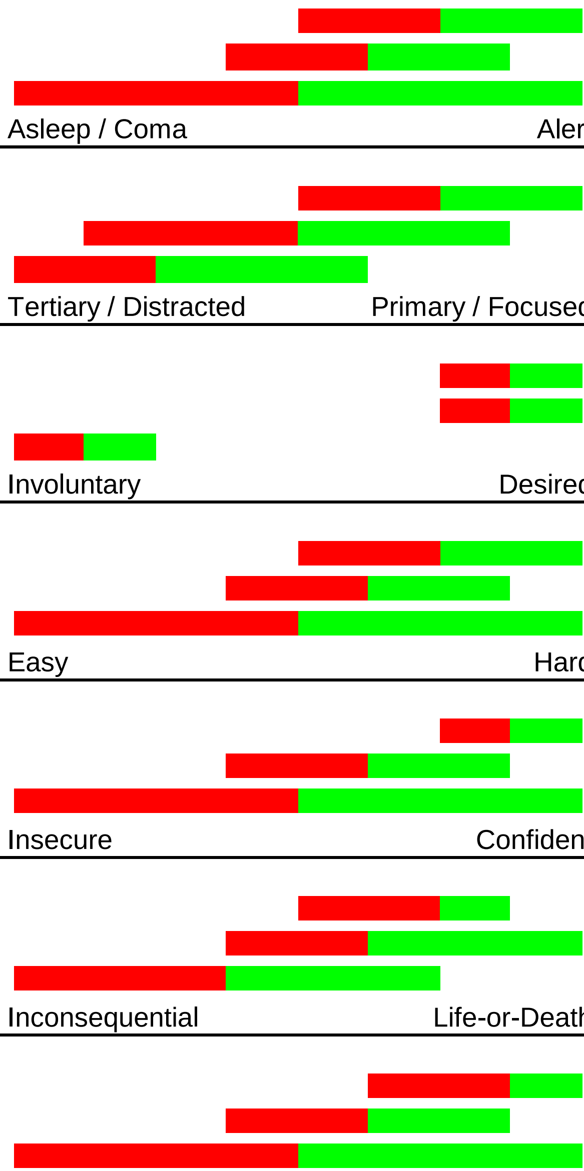
Inputs

(things which affect the outputs)

		glucagon	amylin	carbohydrates	hydration	**insulin**	activity	illness	stress	sleep
Outputs	body weight									
	blood glucose									
	cholesterol									
	triglycerides									

8. Diabetes: anybody, anywhere, anytime

Attribute	Priority	Domain	Range	Notes	Implication	Allocation
Alertness	high	cockpit control room diabetes	Asleep / Coma — Alert	Tasks associated with diabetes are 24x7, whereas other domains - even if they involve shift work - do not involve sleep	Cannot assume they will be awake	Allocate tasks to automation when person is not alert
Attention	high	cockpit control room diabetes	Tertiary / Distracted — Primary / Focused	Tasks associated with diabetes are predominantly secondary (the primary task is "getting on with life"), whereas in other domains the tasks are primary tasks	Cannot assume they are focused	Allocate tasks to automation when person is distracted
Choice	low	cockpit control room diabetes	Involuntary — Desired	The person with diabetes did not choose and does not want the tasks	Cannot assume they want to perform tasks	Allocate tasks to automation which they aren't motivated to perform
Complexity	high	cockpit control room diabetes	Easy — Hard	The tasks associated with diabetes vary greatly in cognitive complexity and memory recall	Cannot assume the tasks are easy / heterogeneous	Allocate simple tasks to automation
Confidence	low	cockpit control room diabetes	Insecure — Confident	People with diabetes range have a great range of self-confidence	Cannot assume they are self-confident	Allocate tasks in such a way as to build confidence
Consequence	medium	cockpit control room diabetes	Inconsequential — Life-or-Death	Consequences of incorrect actions range from inconsequential to life-threatening	Cannot assume tasks are inconsequential	Allocate to automation only low consequence tasks, unless task is very certain
Experience	medium	cockpit control room diabetes	Inexperience — Decades		Cannot assume they are experienced	Allocate tasks to automation without de-skilling



- Type 1 Diabetes
- Artificial Pancreas
- Challenges
- **Applying STPA**

Start with Principles

Governance Principles

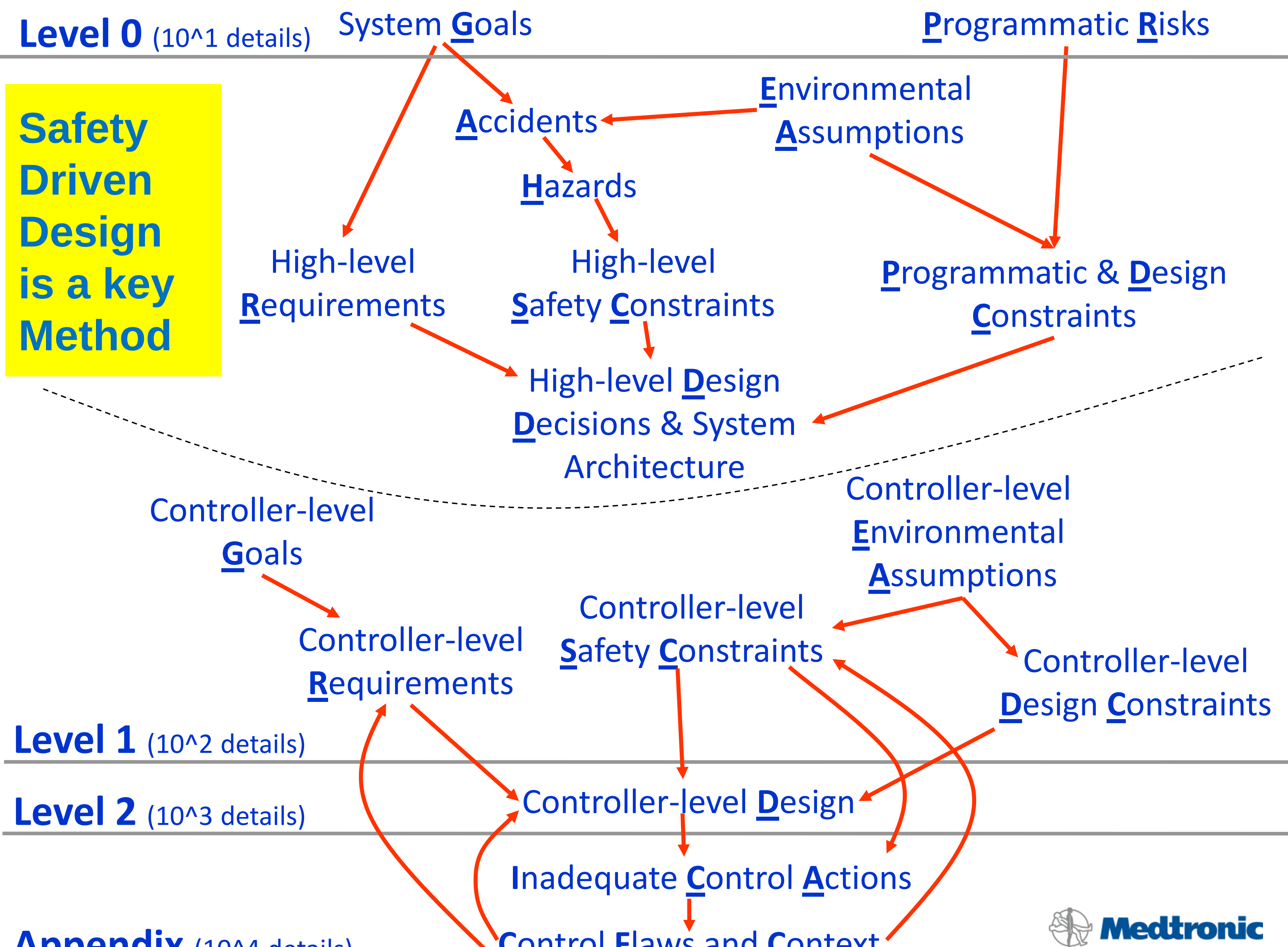
1. We make problems visible
2. We understand customer value
3. We go slow to go fast
4. We collaborate to succeed
5. We deliver value frequently
6. We continuously learn and capture knowledge
7. We manage change

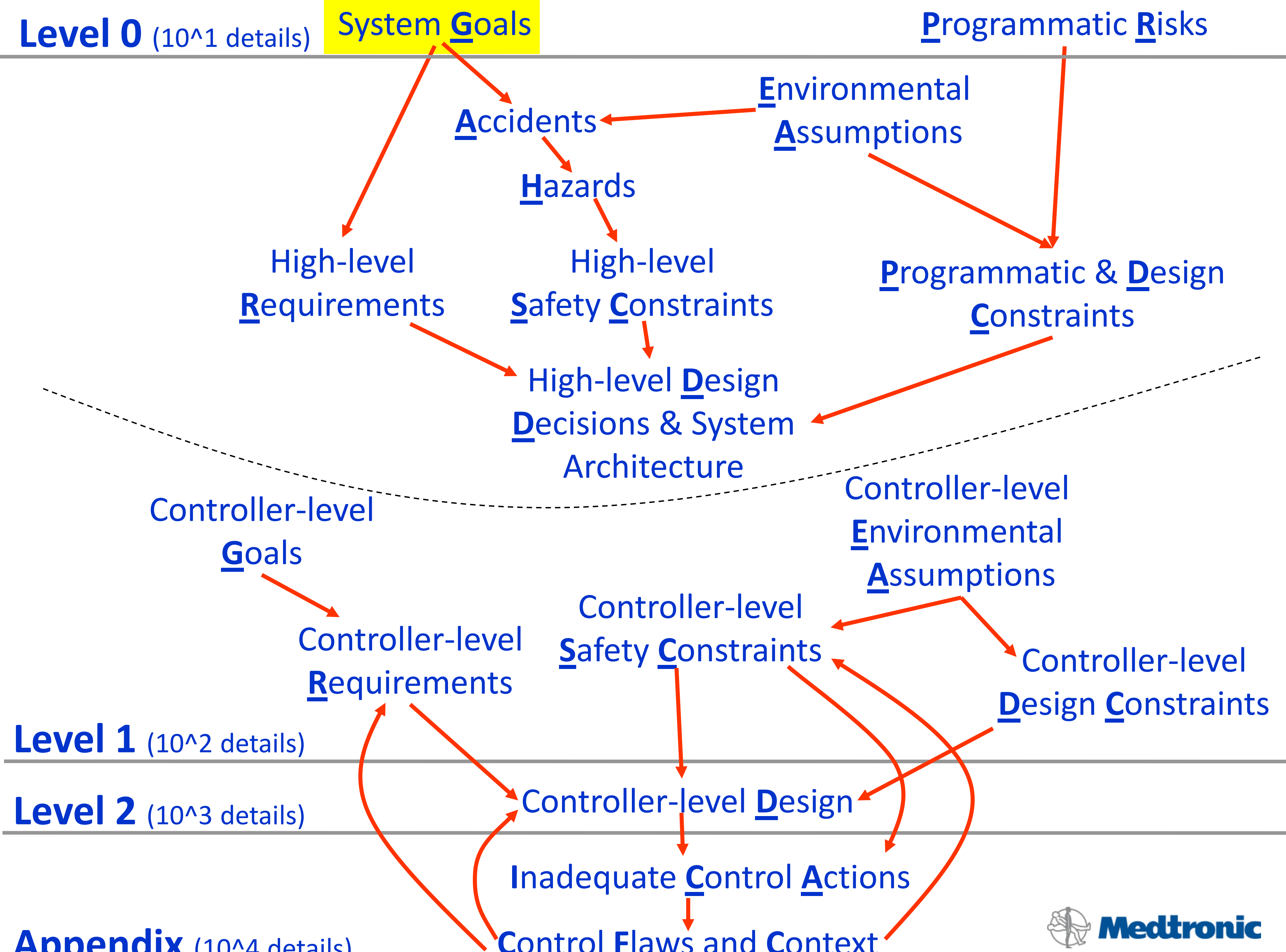
Design Principles

1. We design for dependability
2. We design for simplicity
3. We design for uncertainty
4. We design for human behavior
5. We design for proper task allocation
6. We design for automation supervision
7. We design for automation transparency

Principles Drive Methods

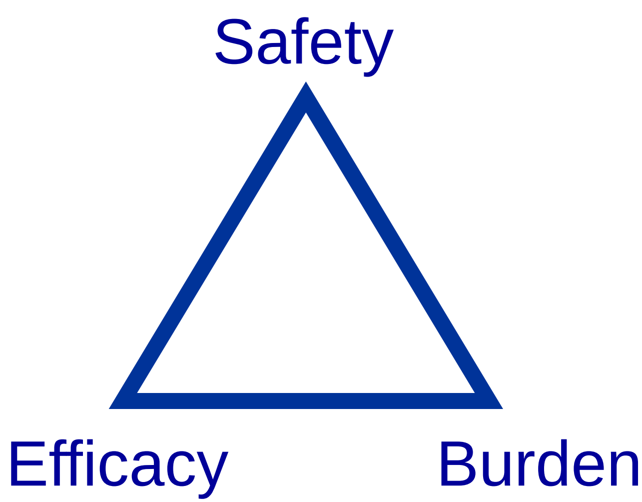
- Lean Development
- Safety Driven Design
- Data Mining
- Modeling-Based Development
- Clinical Trials


Level 0 (10^1 details)
System Goals
Programmatic Risks
Safety Driven Design is a key Method
Accidents
Environmental Assumptions
Hazards
High-level Requirements
High-level Safety Constraints
Programmatic & Design Constraints
High-level Design Decisions & System Architecture
Controller-level Goals
Controller-level Environmental Assumptions
Controller-level Safety Constraints
Controller-level Requirements
Controller-level Design Constraints
Level 1 (10^2 details)
Level 2 (10^3 details)
Controller-level Design
Inadequate Control Actions
Appendix (10^4 details)
Control Flaws and Context
Medtronic


Level 0 (10^1 details)
System Goals
Programmatic Risks
Environmental Assumptions
Accidents
Hazards
High-level Requirements
High-level Safety Constraints
Programmatic & Design Constraints
High-level Design Decisions & System Architecture
Controller-level Goals
Controller-level Environmental Assumptions
Controller-level Safety Constraints
Controller-level Requirements
Controller-level Design Constraints
Level 1 (10^2 details)
Level 2 (10^3 details)
Controller-level Design
Inadequate Control Actions
Appendix (10^4 details)
Control Flaws and Context
Medtronic

Goal: Commercialize a next generation artificial pancreas which is:

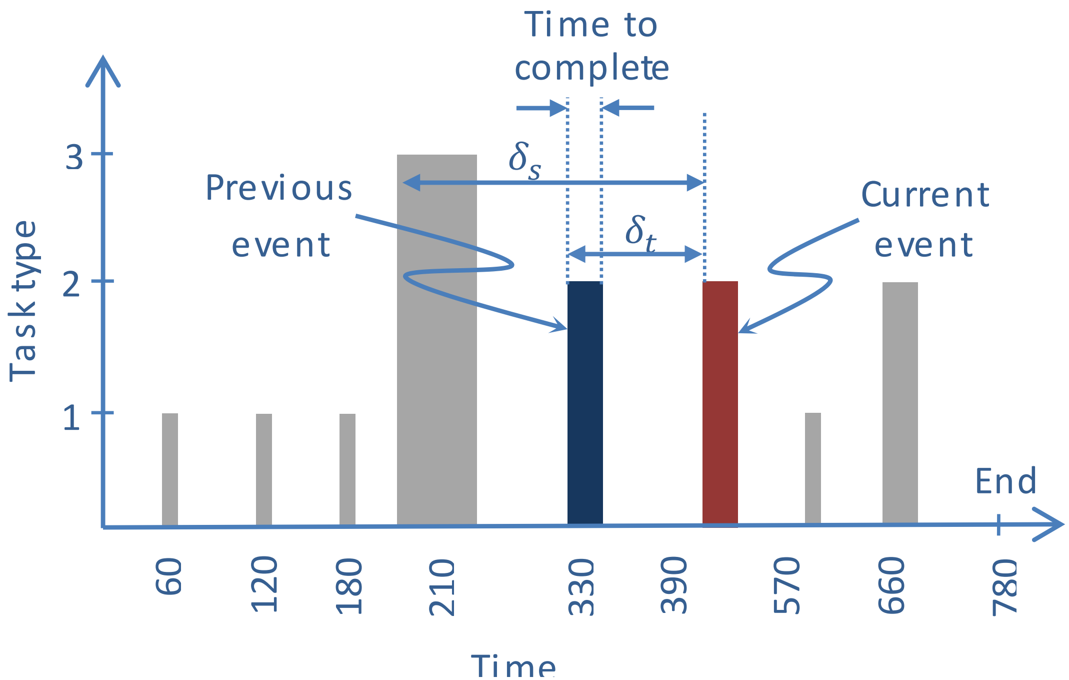
1. Less burdensome
2. More effective
3. Safe



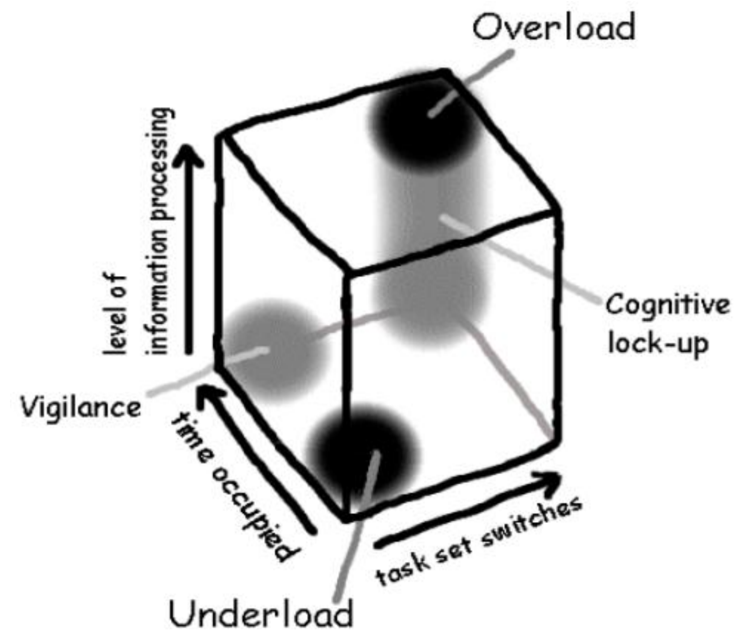
Medtronic

Quantifying Burden

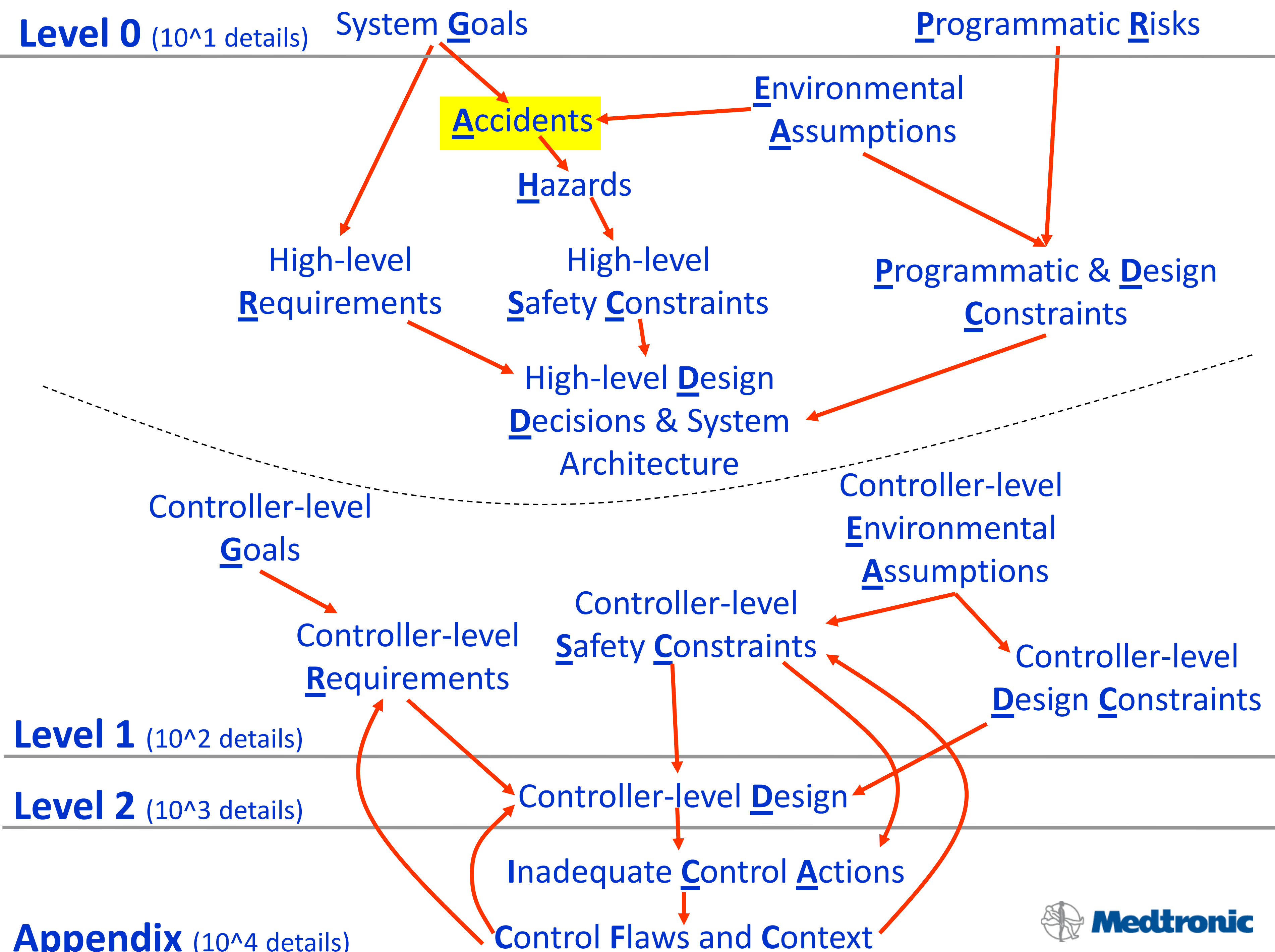
Time Series of Events, alarms, actions



Overload, Vigilance Cognitive lock-up



Burden = *f*(Overload, Vigilance, Cognitive lock-up)


Level 0 (10^1 details)
System Goals
Programmatic Risks
Environmental Assumptions
Accidents
Hazards
High-level Requirements
High-level Safety Constraints
Programmatic & Design Constraints
High-level Design Decisions & System Architecture
Controller-level Goals
Controller-level Environmental Assumptions
Controller-level Safety Constraints
Controller-level Requirements
Controller-level Design Constraints
Level 1 (10^2 details)
Level 2 (10^3 details)
Controller-level Design
Inadequate Control Actions
Appendix (10^4 details)
Control Flaws and Context

Accidents

Accidents, or Loss Events, are those things that *must not* happen in efforts to satisfy system goals.

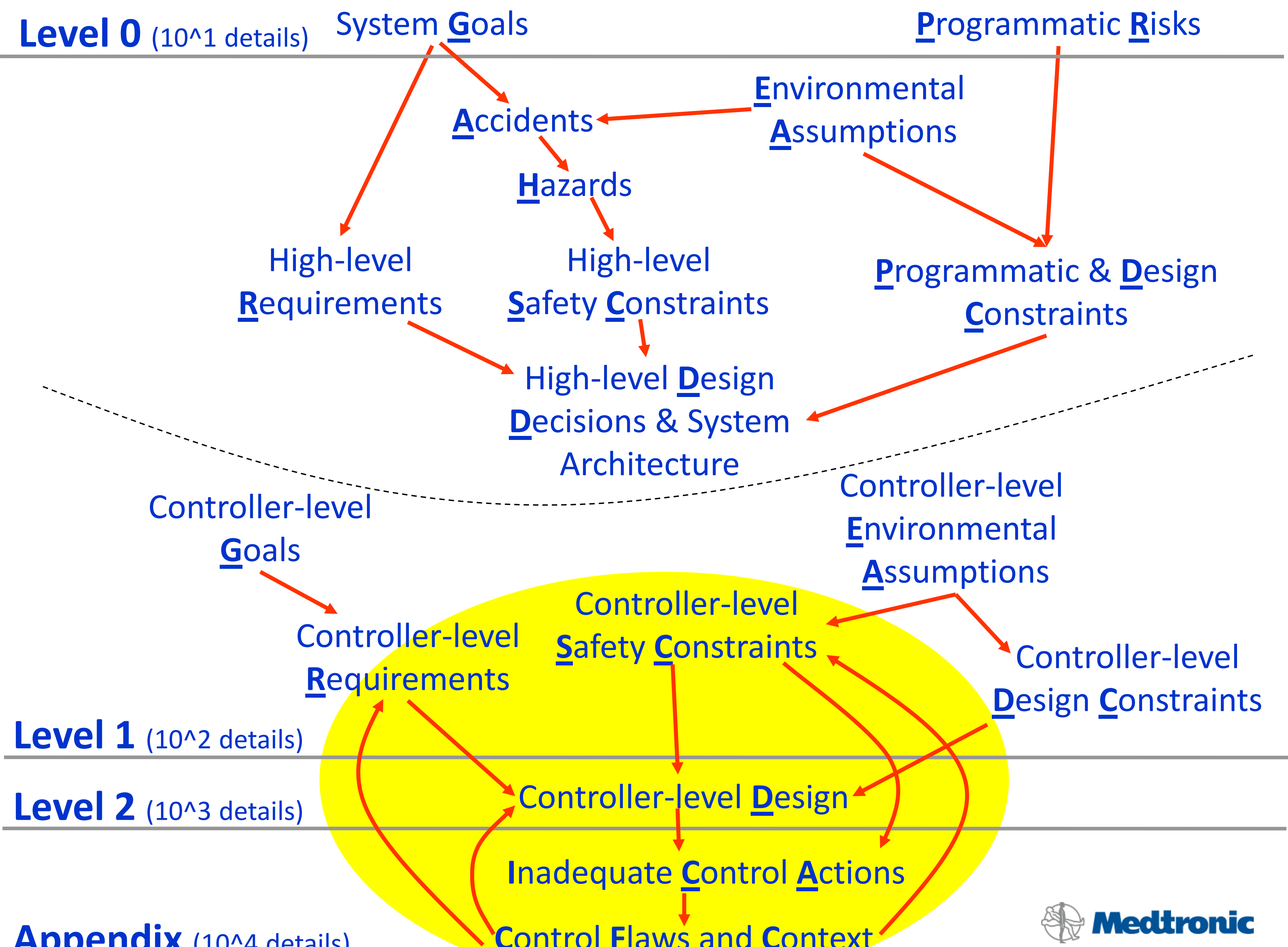
Example:

ACC.1 Acute incident of hypoglycemia

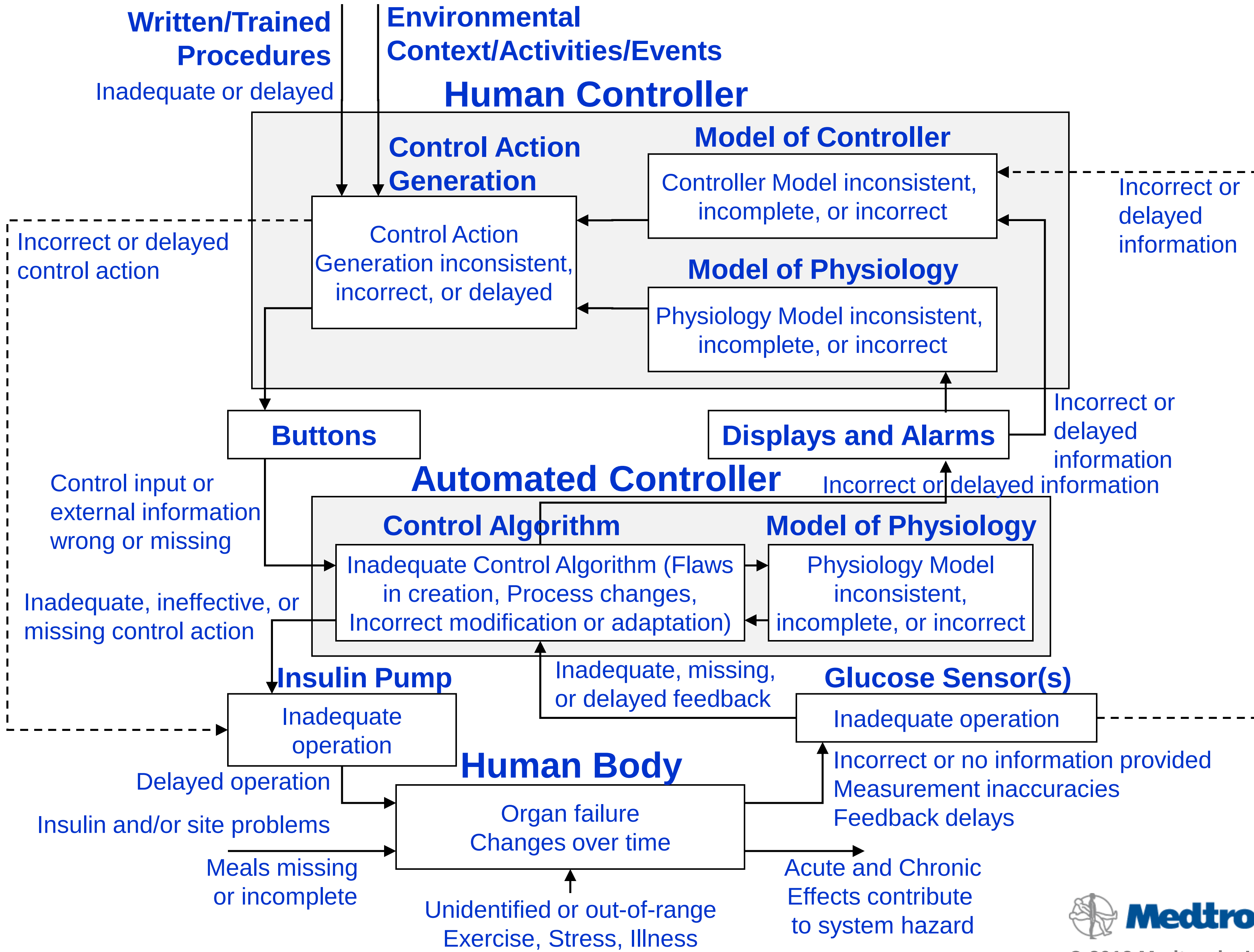
ACC.2 Acute incident of hyperglycemia

ACC.3 Chronic hyperglycemia

ACC.4 Patient ceases effective therapy


Level 0 (10^1 details)
System Goals
Programmatic Risks
Environmental Assumptions
Accidents
Hazards
High-level Requirements
High-level Safety Constraints
Programmatic & Design Constraints
High-level Design Decisions & System Architecture
Controller-level Goals
Controller-level Environmental Assumptions
Controller-level Safety Constraints
Controller-level Requirements
Controller-level Design Constraints
Level 1 (10^2 details)
Level 2 (10^3 details)
Controller-level Design
Inadequate Control Actions
Appendix (10^4 details)
Control Flaws and Context
Medtronic

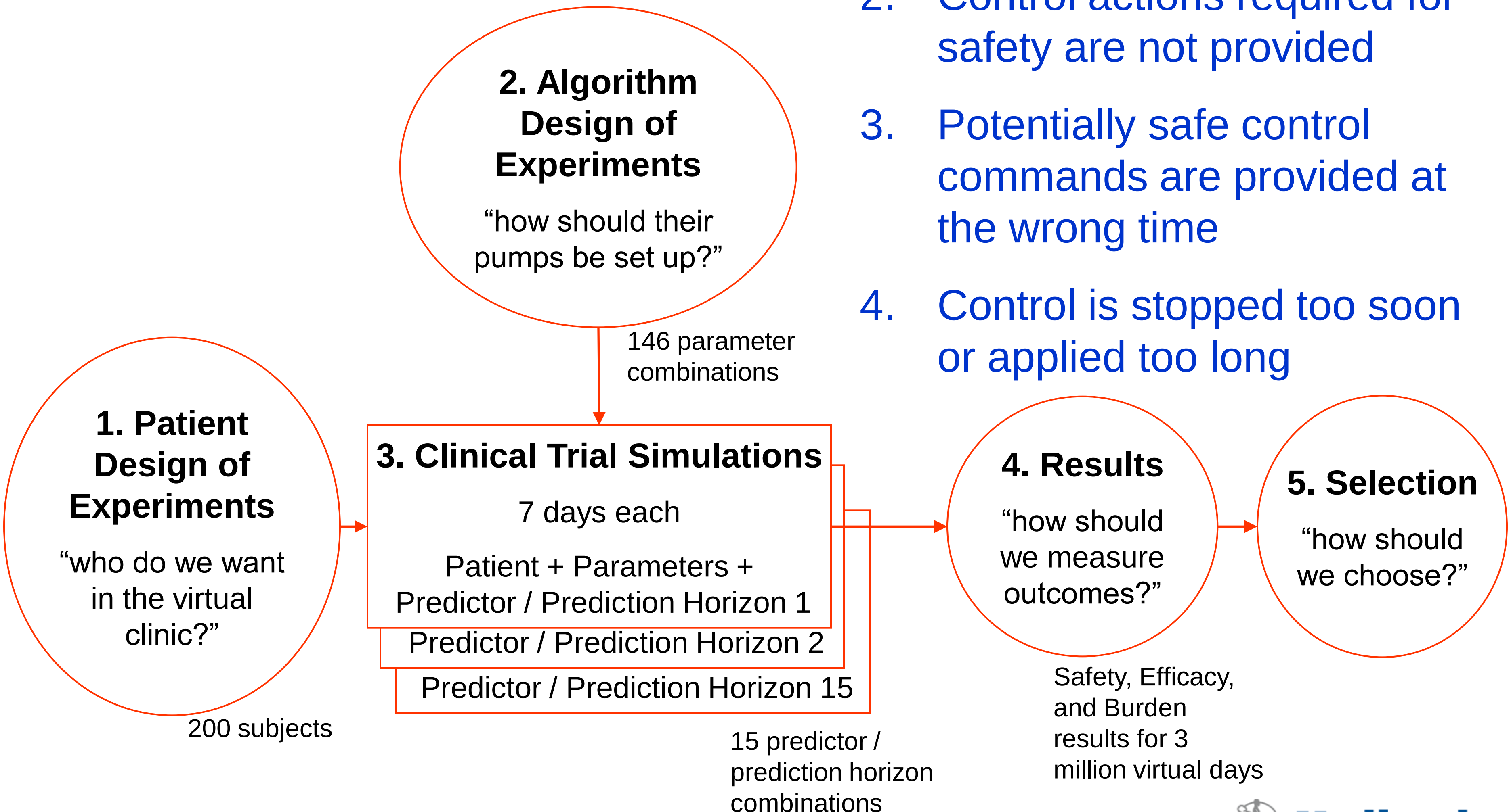
Inadequate Control Actions (ICA's)



Medtronic

Model-Based Development fosters STPA

1. Unsafe control commands are given
2. Control actions required for safety are not provided
3. Potentially safe control commands are provided at the wrong time
4. Control is stopped too soon or applied too long



Medtronic

Example Result

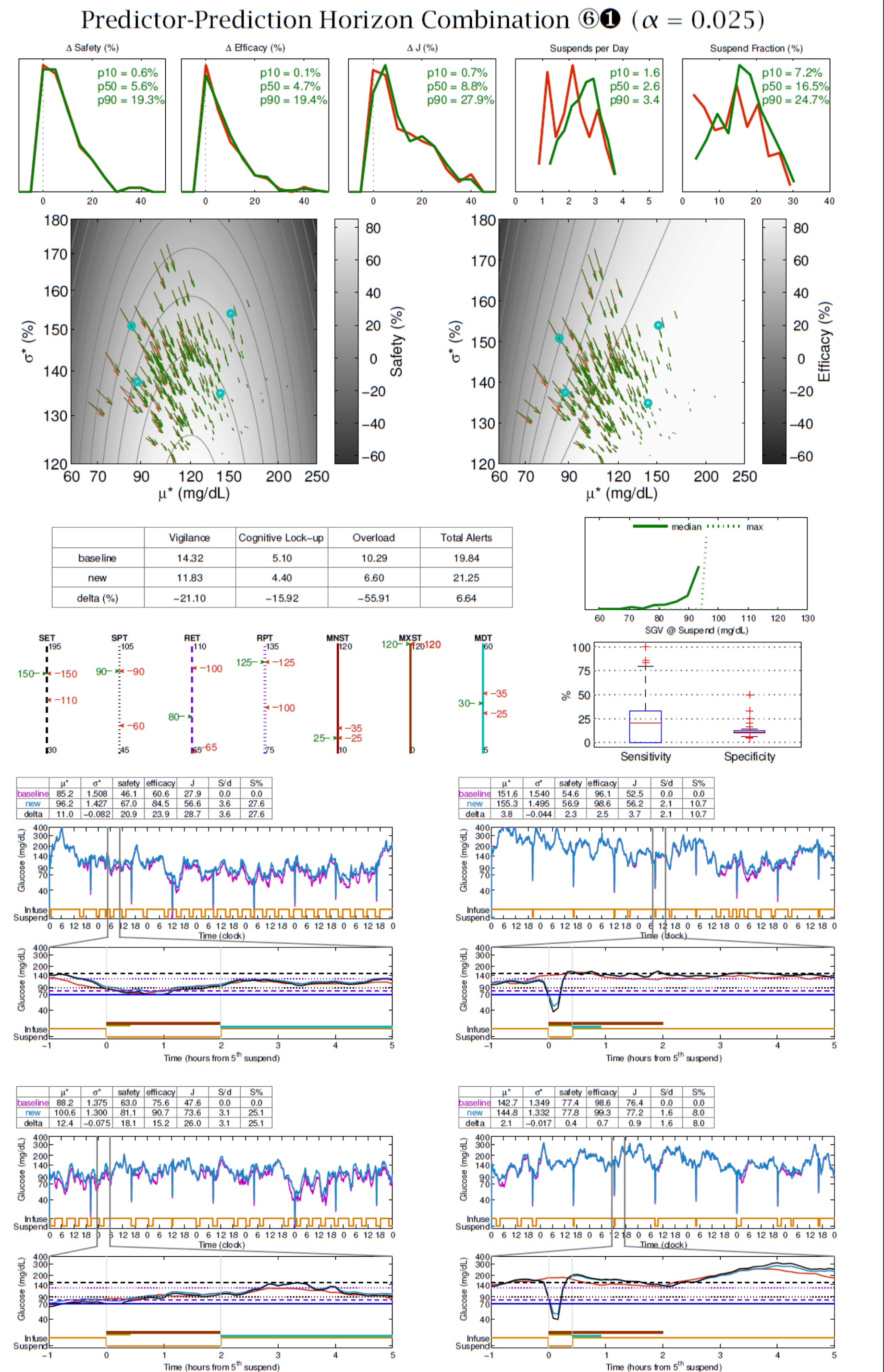
100 virtual subjects

x 2 trials per subject

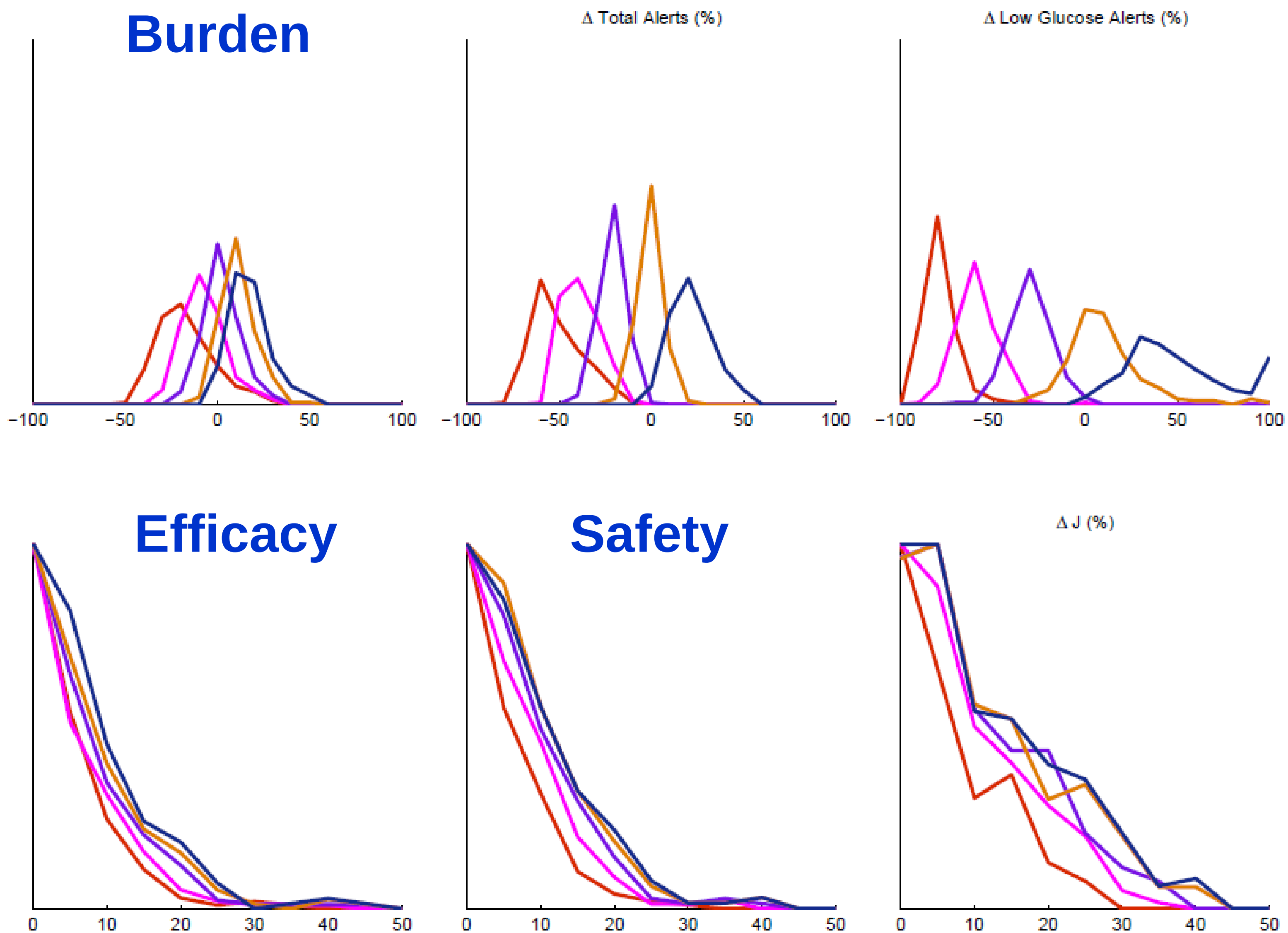
x 7 days per trial

x 2206 experiments / subject

= 3 million subject-days

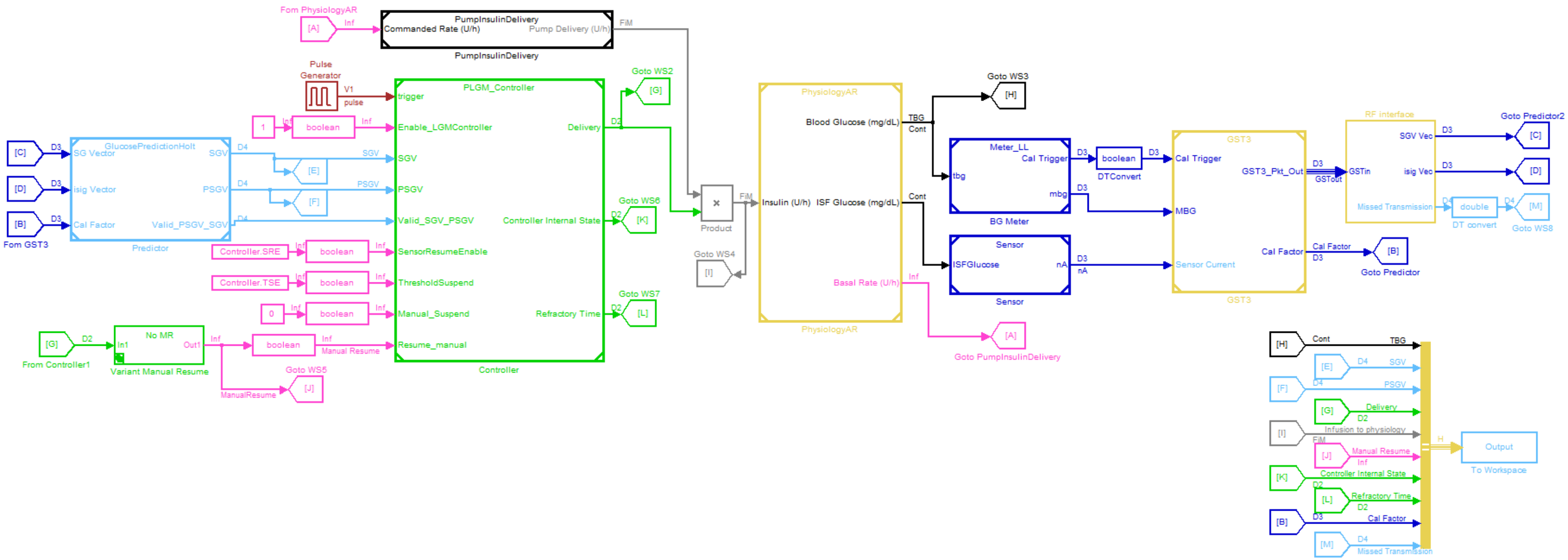


Safety, Efficacy, Burden – Trade Analysis



Medtronic

Executable Specification / Model-Based Development



Requirements Specification

Medtronic

Low Glucose Control in NGP

Subsystem Requirements Specification (SSyRS)

VERSION: 1.0

REVISION DATE: 02/24/2012

Summary

1. Diabetes control is complex
2. Artificial Pancreas is a series of steps
3. Diabetes is a perfect fit for STPA
4. We have started the journey

Lane.Desborough
@Medtronic.com

Medtronic