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

A Systems Engineering Approach

Lane Desborough, Product Strategist

www.diabetesartday.com

Life with Diabetes is not easy!
Blood Glucose

Insulin Delivery

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
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

Sense  →  Decide  →  Act

algorithm

© 2012 Medtronic, Inc.
Artificial Pancreas: safely transfer variation from blood glucose to insulin in order to make living with diabetes easier.

Without diabetes:
- Glucose: 90±15

Single daily injection:
- Glucose: 170±100

Multiple daily injections:
- Glucose: 150±70

Pump basal and bolus:
- Glucose: 130±50

Closed loop:
- Glucose: 110±30

Diabetes injections:
- Pancreatic insulin
- Slow-acting insulin
- Slow- and fast-acting insulin
- Fast-acting insulin

© 2012 Medtronic, Inc.
Type 1 Diabetes
Artificial Pancreas
Challenges
Applying STPA
1. There are many **sources** of variation

<table>
<thead>
<tr>
<th>Timing</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every 3-7 years</td>
<td>1. Complications</td>
</tr>
<tr>
<td></td>
<td>2. Physiological changes</td>
</tr>
<tr>
<td>Every year</td>
<td>3. Serious events</td>
</tr>
<tr>
<td></td>
<td>4. Illness stress</td>
</tr>
<tr>
<td>Every quarter</td>
<td>5. Travel / time zone changes</td>
</tr>
<tr>
<td></td>
<td>6. Psychological stress</td>
</tr>
<tr>
<td>Every week</td>
<td>7. Missed meals</td>
</tr>
<tr>
<td>Every 3 days</td>
<td>8. Restaurant meals</td>
</tr>
<tr>
<td>Every meal</td>
<td>9. Hormonal stress</td>
</tr>
<tr>
<td>Every hour</td>
<td>10. Psychological stress</td>
</tr>
<tr>
<td>Every minute</td>
<td>11. Circadian rhythms</td>
</tr>
<tr>
<td></td>
<td>12. Exercise stress</td>
</tr>
<tr>
<td></td>
<td>13. Normal meals</td>
</tr>
<tr>
<td></td>
<td>14. Movement</td>
</tr>
</tbody>
</table>
2. There is a limit to how much variation *can* be transferred

~25-40 min delay

Artificial Pancreas
3. There isn’t consensus on \textit{which} variation to transfer (which loss function to use)
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

© 2012 Medtronic, Inc.
5. There are challenges in Sensing, Deciding, and Acting

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

<table>
<thead>
<tr>
<th>Sensor Site</th>
<th>Sensor</th>
<th>Transmitter</th>
<th>Calibration</th>
<th>Sensor Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressed, Fatigued, Slow Dynamics</td>
<td>Pulled out, Old, Noisy, Disconnected, Drifting, Biased, Non-linear</td>
<td>Dead battery, Wireless blocked, Wireless spoofed</td>
<td>Outdated strips, Contaminated fingers, Missed</td>
<td>Inaccurate, Missing, Deadtime, Lag, Dead battery,</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Insulin</th>
<th>Pump</th>
<th>Infusion Set</th>
<th>Infusion Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong kind, Slow acting, Degraded (old, fried), Air entrained</td>
<td>Wrong bolus type, Wrong bolus amount, Dead battery</td>
<td>Occlusion, Cold, Disconnected, Air-in-line</td>
<td>Compressed, Fatigued, Intramuscular, intravenous, Pulled-out, Slow Dynamics</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Inputs (things which affect the outputs)</th>
<th>glucagon</th>
<th>amylin</th>
<th>carbohydrates</th>
<th>hydration</th>
<th>insulin</th>
<th>activity</th>
<th>illness</th>
<th>stress</th>
<th>sleep</th>
</tr>
</thead>
<tbody>
<tr>
<td>body weight</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>blood glucose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cholesterol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>triglycerides</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2012 Medtronic, Inc.
## 8. Diabetes: anybody, anywhere, anytime

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

© 2012 Medtronic, Inc.
- 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
Safety Driven Design is a key Method

System Goals

Accidents

Hazard

High-level Requirements

High-level Design Decisions & System Architecture

Controller-level Goals

Controller-level Safety Constraints

Controller-level Design Constraints

Controller-level Environmental Assumptions

Programmatic & Design Constraints

Programmatic Risks

Environmental Assumptions

Level 0 (10^1 details)

Level 1 (10^2 details)

Level 2 (10^3 details)

Appendix (10^4 details)
Goal: Commercialize a next generation artificial pancreas which is:

1. Less burdensome
2. More effective
3. Safe
Quantifying Burden

Time Series of Events, alarms, actions

Time to complete

Overload, Vigilance
Cognitive lock-up

Burden = f(Overload, Vigilance, Cognitive lock-up)
Level 0 (10^1 details)

System Goals

High-level Requirements

Accidents

Environmental Assumptions

Programmatic Risks

Level 1 (10^2 details)

High-level Safety Constraints

Controller-level Goals

Controller-level Requirements

Controller-level Design

Controller-level Environmental Assumptions

Controller-level Design Constraints

Level 2 (10^3 details)

Controller-level Safety Constraints

Inadequate Control Actions

Control Flaws and Context

Appendix (10^4 details)
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
Inadequate Control Actions (ICA’s)

- **Written/Trained Procedures**
  - Inadequate or delayed control action

- **Human Controller**
  - **Control Action Generation**
    - Inadequate operation
  - **Model of Controller**
    - Controller Model inconsistent, incomplete, or incorrect
  - **Model of Physiology**
    - Physiology Model inconsistent, incomplete, or incorrect

- **Automated Controller**
  - **Control Algorithm**
    - Inadequate Control Algorithm (Flaws in creation, Process changes, Incorrect modification or adaptation)
  - **Model of Physiology**
    - Physiology Model inconsistent, incomplete, or incorrect

- **Insulin Pump**
  - Inadequate operation
  - Delayed operation
  - Insulin and/or site problems
  - Meals missing or incomplete

- **Human Body**
  - Organ failure
  - Changes over time
  - Unidentified or out-of-range Exercise, Stress, Illness

- **Displays and Alarms**
  - Inadequate, missing, or delayed feedback
  - Incorrect or delayed information

- **Glucose Sensor(s)**
  - Incorrect or no information provided
  - Measurement inaccuracies
  - Feedback delays

- **Human Context/Activities/Events**
  - Inadequate or delayed control action

- **Buttons**
  - Control input or external information wrong or missing

- **Inadequate Control Algorithm (ICA’s)**
  - Inadequate, ineffective, or missing control action
  - Incorrect or delayed control action

- **Unidentified or out-of-range**
  - Exercise, Stress, Illness

- **Acute and Chronic Effects contribute to system hazard**
Model-Based Development fosters STPA

1. Patient Design of Experiments
   “who do we want in the virtual clinic?”

2. Algorithm Design of Experiments
   “how should their pumps be set up?”
   - 146 parameter combinations

3. Clinical Trial Simulations
   7 days each
   - Patient + Parameters + Predictor / Prediction Horizon 1
   - Predictor / Prediction Horizon 2
   - Predictor / Prediction Horizon 15
   - 200 subjects
   - 15 predictor / prediction horizon combinations

4. Results
   “how should we measure outcomes?”
   - Safety, Efficacy, and Burden results for 3 million virtual days

5. Selection
   “how should we choose?”

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

© 2012 Medtronic, Inc.
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

Burden

Efficacy

Safety

Δ Total Alerts (%)

Δ Low Glucose Alerts (%)

Δ J (%)
Executable Specification / Model-Based Development
Requirements Specification

Low Glucose Control in NGP

Subsystem Requirements Specification (SSyRS)

VERSION: 1.0

REVISED 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