Automated Insulin Delivery

Lane Desborough
Co-founder and Chief Engineer, Bigfoot Biomedical

Disclaimer and Disclosure

- Lane Desborough is an employee of Bigfoot Biomedical, Inc.
- Bigfoot Biomedical, Inc. does not market or sell any medical devices.
- This presentation was prepared by Lane Desborough in his personal capacity. The opinions expressed in this article are the author's own and do not reflect the view of Bigfoot Biomedical, Inc.

Lane Desborough

1992 M.Sc. Chemical Engineering (Process Control), Queen's University, "Performance Assessment Measures for Univariate Control"

1990 B.A.Sc. Chemical Engineering with Management Sciences Option, University of Waterloo

MISTAKES

It Could Be that the Purpose of Your Life Is Only to Serve as a Warning to Others.

Despair.com

What is this?

1. It cost billions of dollars to build, operate, and maintain
2. It is in some way unique and has no identical twin
3. It is one of the most complex systems in the world
4. It's but one part of a larger system
5. It deals with incredibly hazardous situations, 24x7
6. It provides something which society must have to survive
7. It employs hundreds of professionals from many disciplines
8. Its ongoing operation involves thousands of complex tasks
9. It's subject to ever changing conditions in the environment
10. It adapts and changes over a multidecade life
11. It is incredibly safe, reliable, secure, and efficient

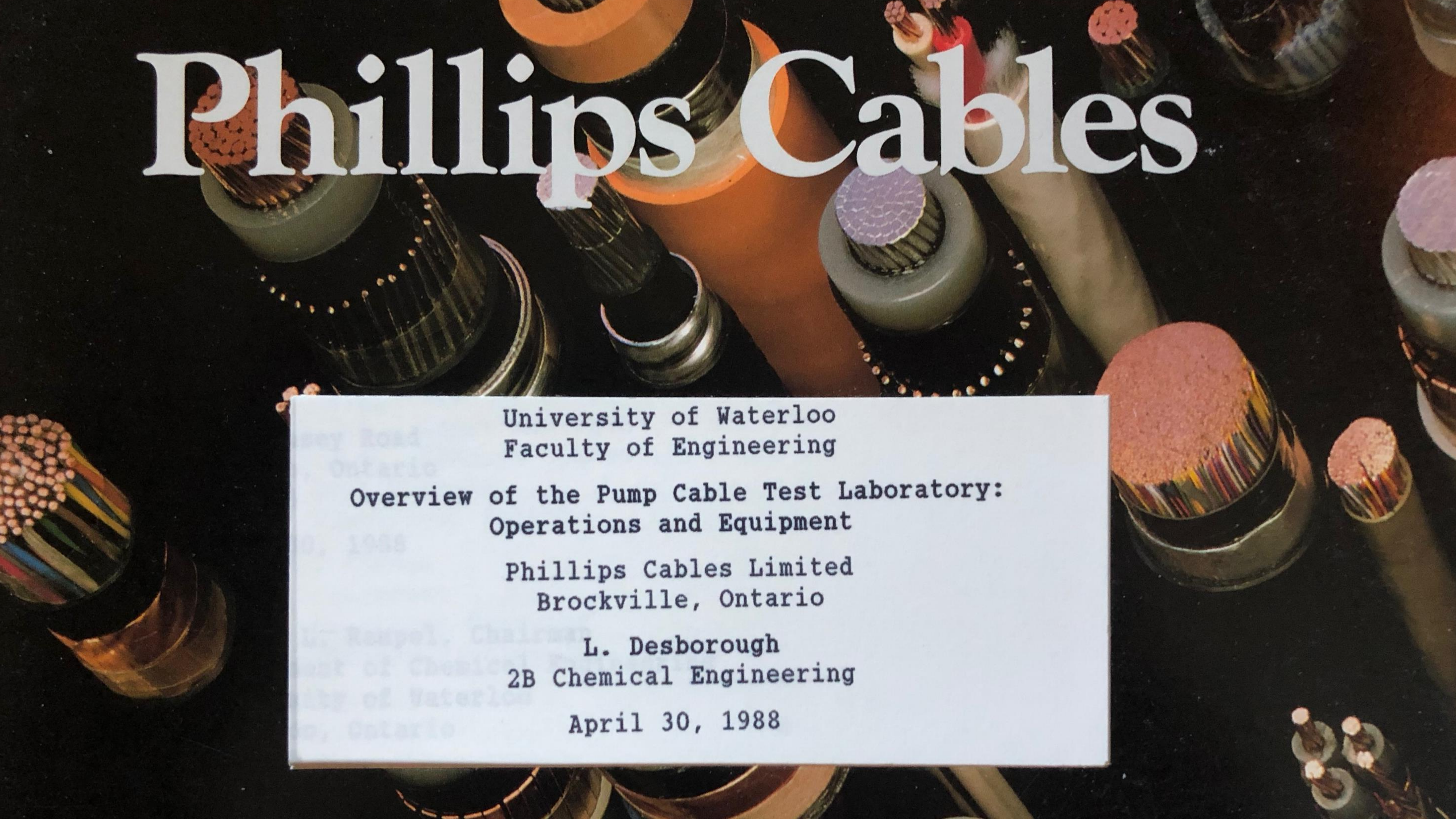




SINGAPORE AIRLINES

CARPOOLS
ONLY
LEFT LANE


My first cyberphysical system



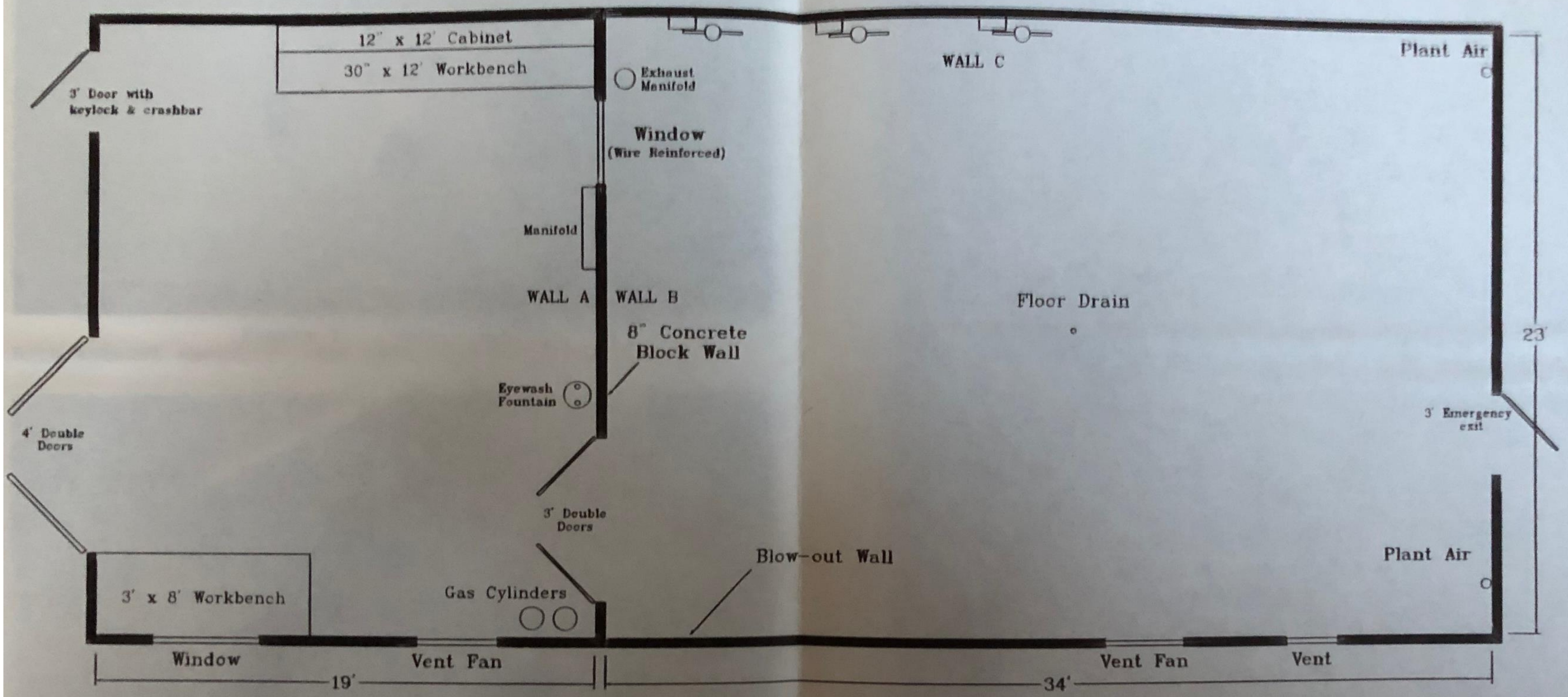
University of Waterloo
Faculty of Engineering

Overview of the Pump Cable Test Laboratory: Operations and Equipment

Phillips Cables Limited
Brockville, Ontario

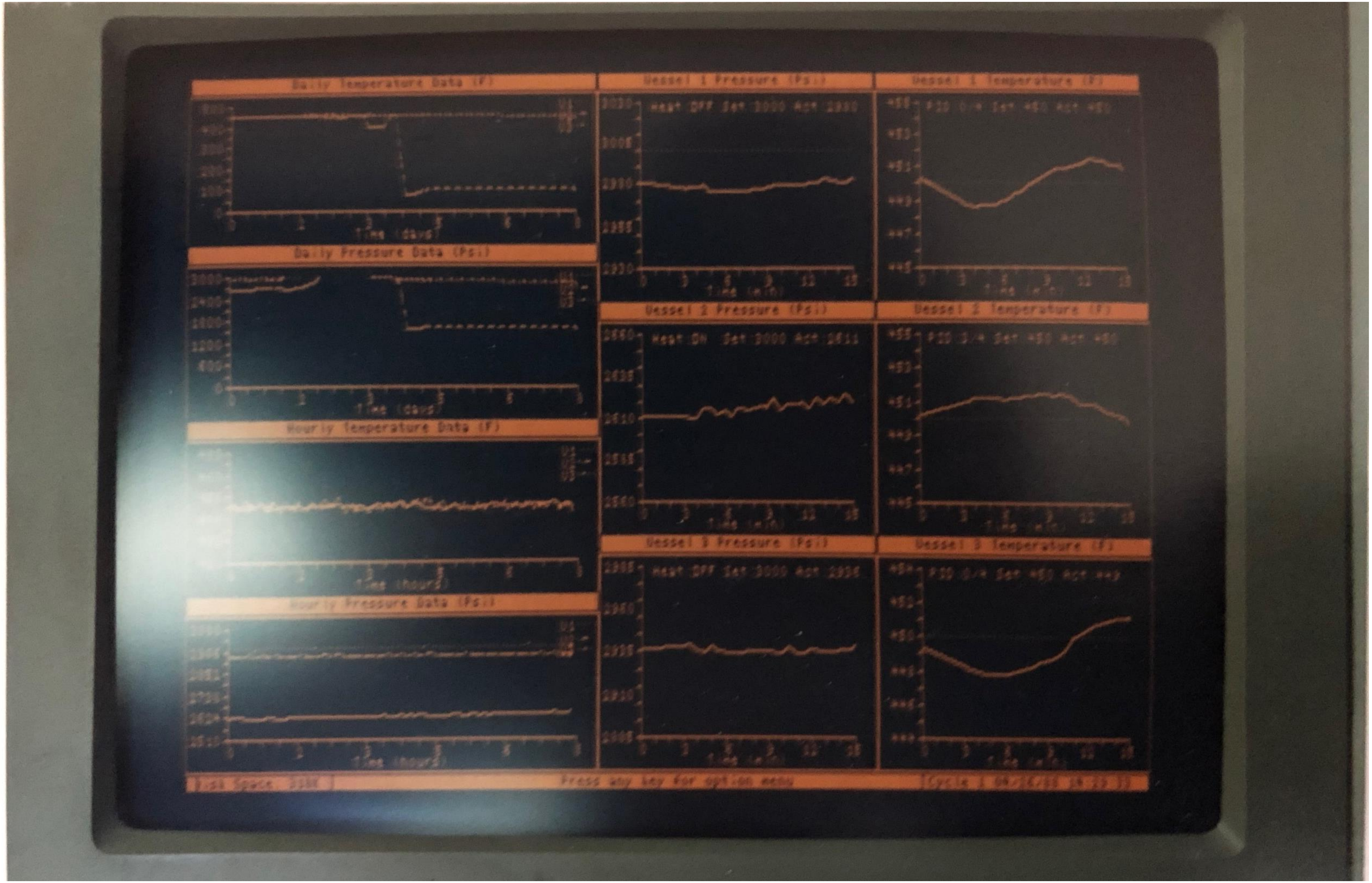
L. Desborough
2B Chemical Engineering

April 30, 1988



Phillips Cables LIMITED

Pump Cable Test Facility	SCALE:	DRAWN BY: L. Desborough
OVERALL LAYOUT		
DATE: 88/02/15	REVISION 2	DRAWING NUMBER: PCTL-1



Daily Temperature Data (F)
Vessel 1 Pressure (Psi)
Vessel 1 Temperature (F)
Daily Pressure Data (Psi)
Vessel 2 Pressure (Psi)
Vessel 2 Temperature (F)
Hourly Temperature Data (F)
Vessel 3 Pressure (Psi)
Vessel 3 Temperature (F)
Hourly Pressure Data (Psi)
Time (days)
Time (hours)
Time (min)
Press any key for option menu


REC
REC
REC

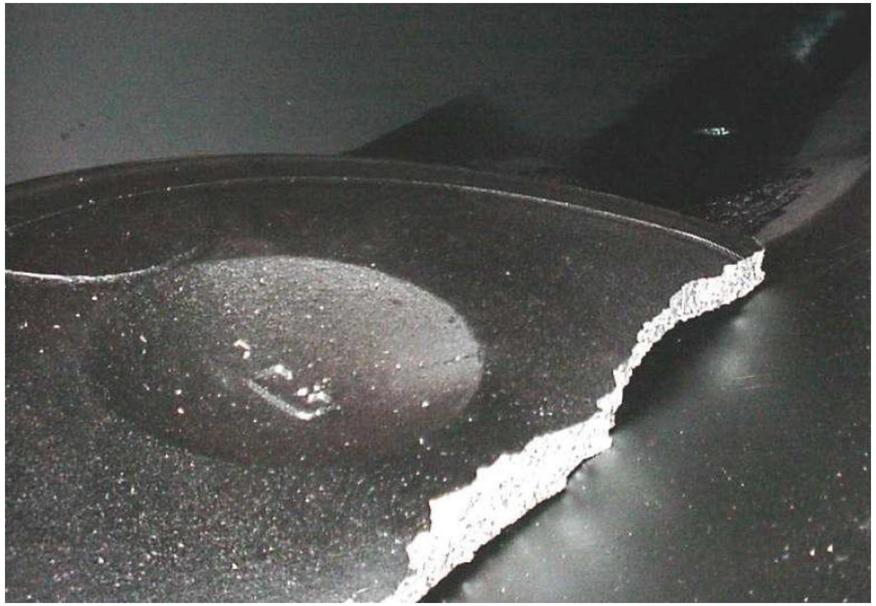
My second cyberphysical system


6,000,000,000
5,000
15

- Process Modeling
- Basic Control
- Advanced Control
- Statistical Data Analysis
- Operations Support
- Human-Machine Interfaces
- Real Time Optimization
- Control System Modernization

Bad things can happen during mode transitions, when the state of the system is changing.

Software is a harmless mental abstraction until it is instantiated in the physical world

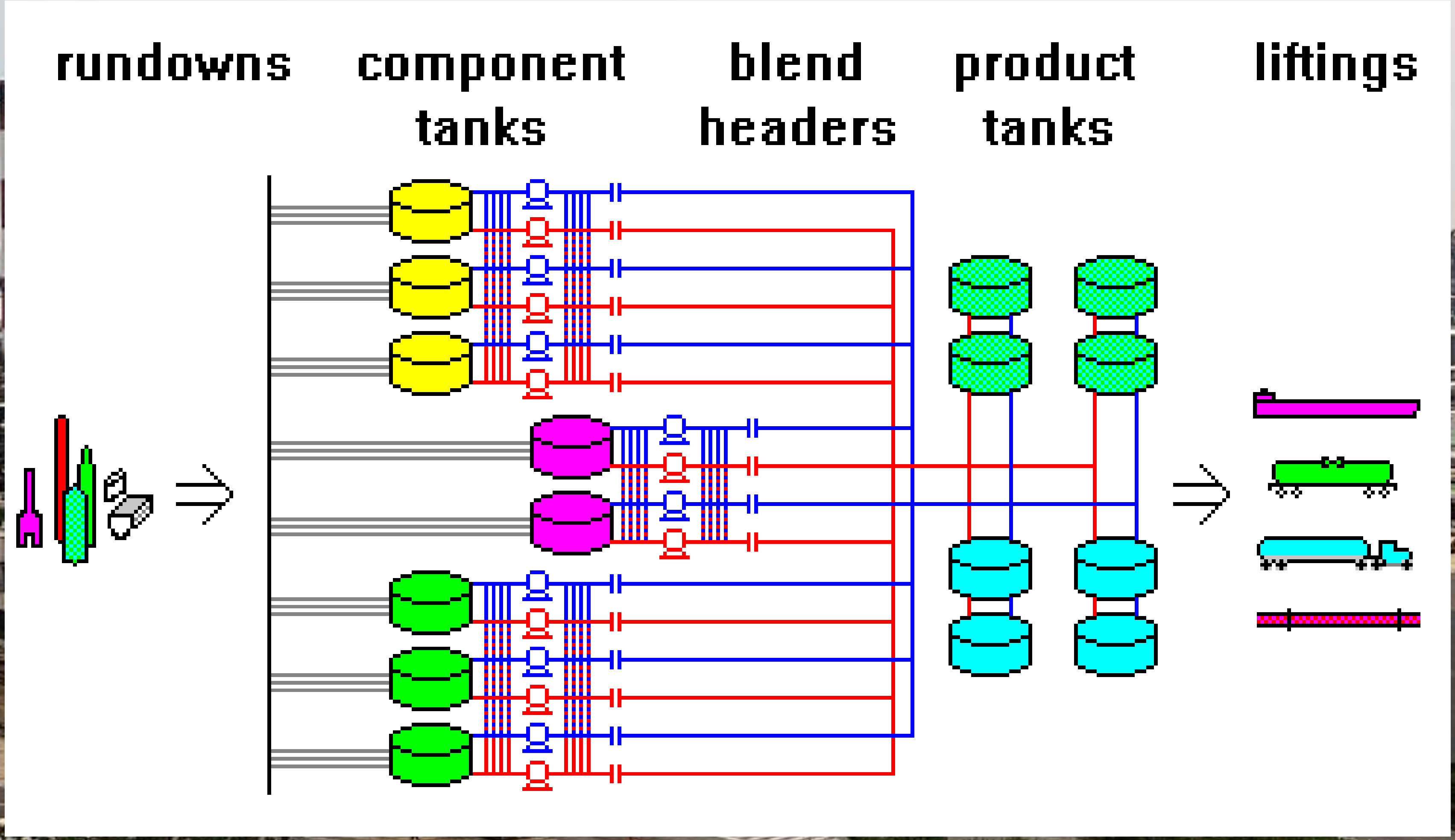


David Gent, “Software Upgrade Triggers Events that Lead to Plant Shutdown”, AIChE Ethylene producers' conference; 2004; New Orleans, La16; 542-563

My third cyberphysical system

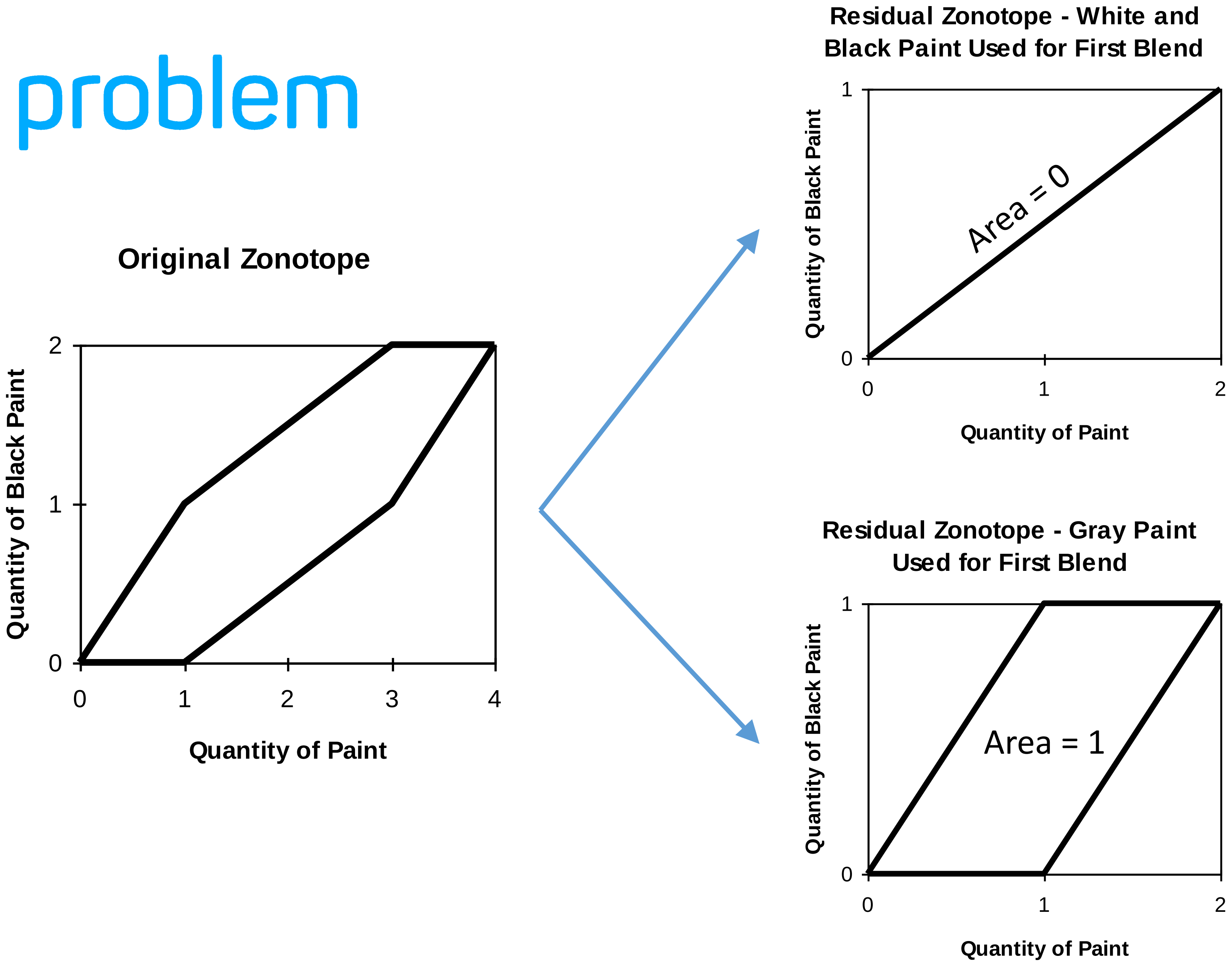
Ulsan refinery is the third largest oil refinery in the world with a capacity of 840,000bpd. It is located in Ulsan Metropolitan City in South Korea and is owned by SK Energy. The refinery produces LPG, gasoline, diesel, jet fuel and asphalt.

Ulsan refinery is the third largest oil refinery in the world with a capacity of 840,000bpd. It is located in Ulsan Metropolitan City in South Korea and is owned by SK Energy. The refinery produces LPG, gasoline, diesel, jet fuel and asphalt.



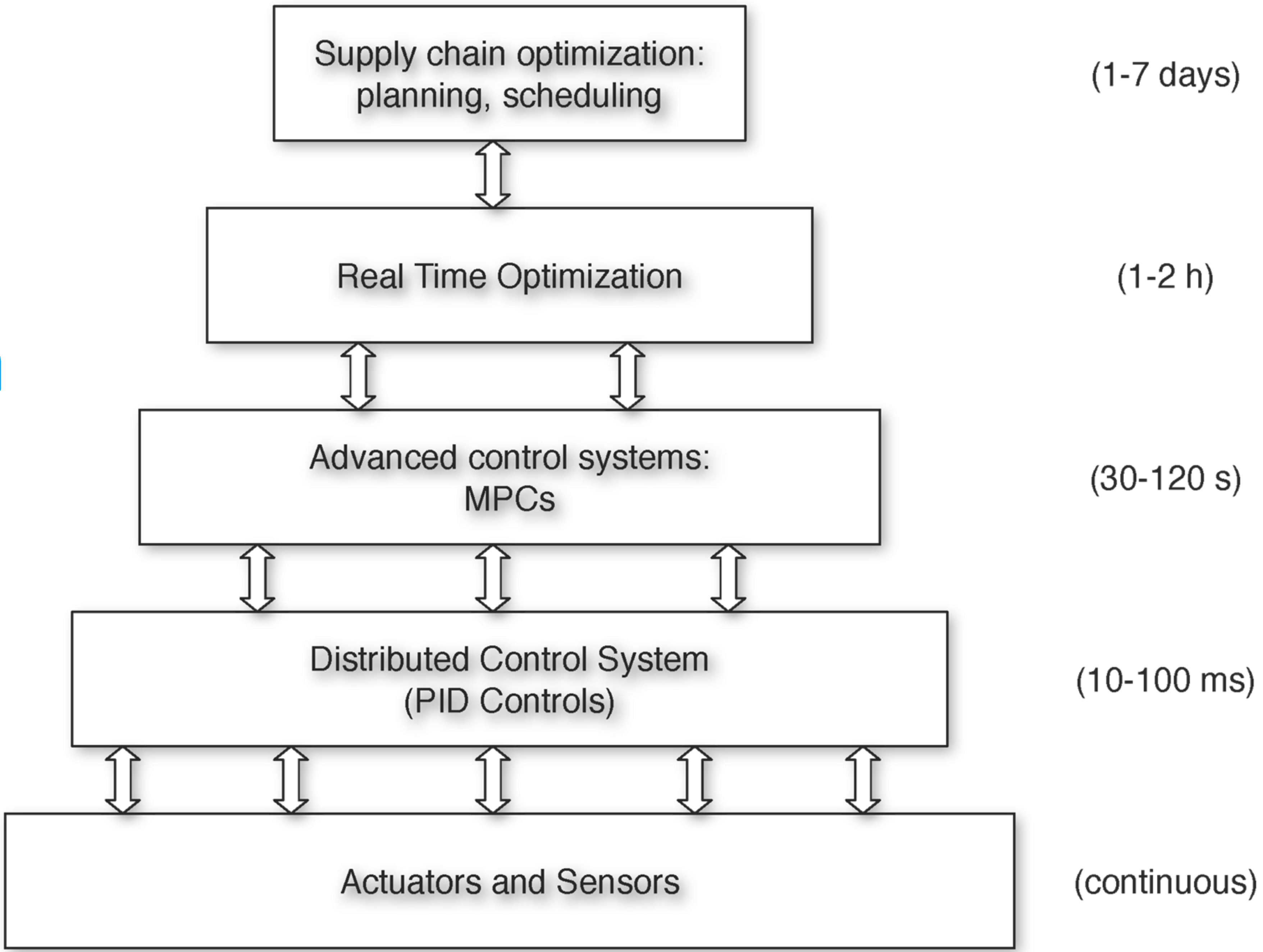
Paint dealer problem

White	Gray	Black
1 gal	2 gal	1 gal
Cost 10$/gal	Cost 12$/gal	Cost 9$/gal



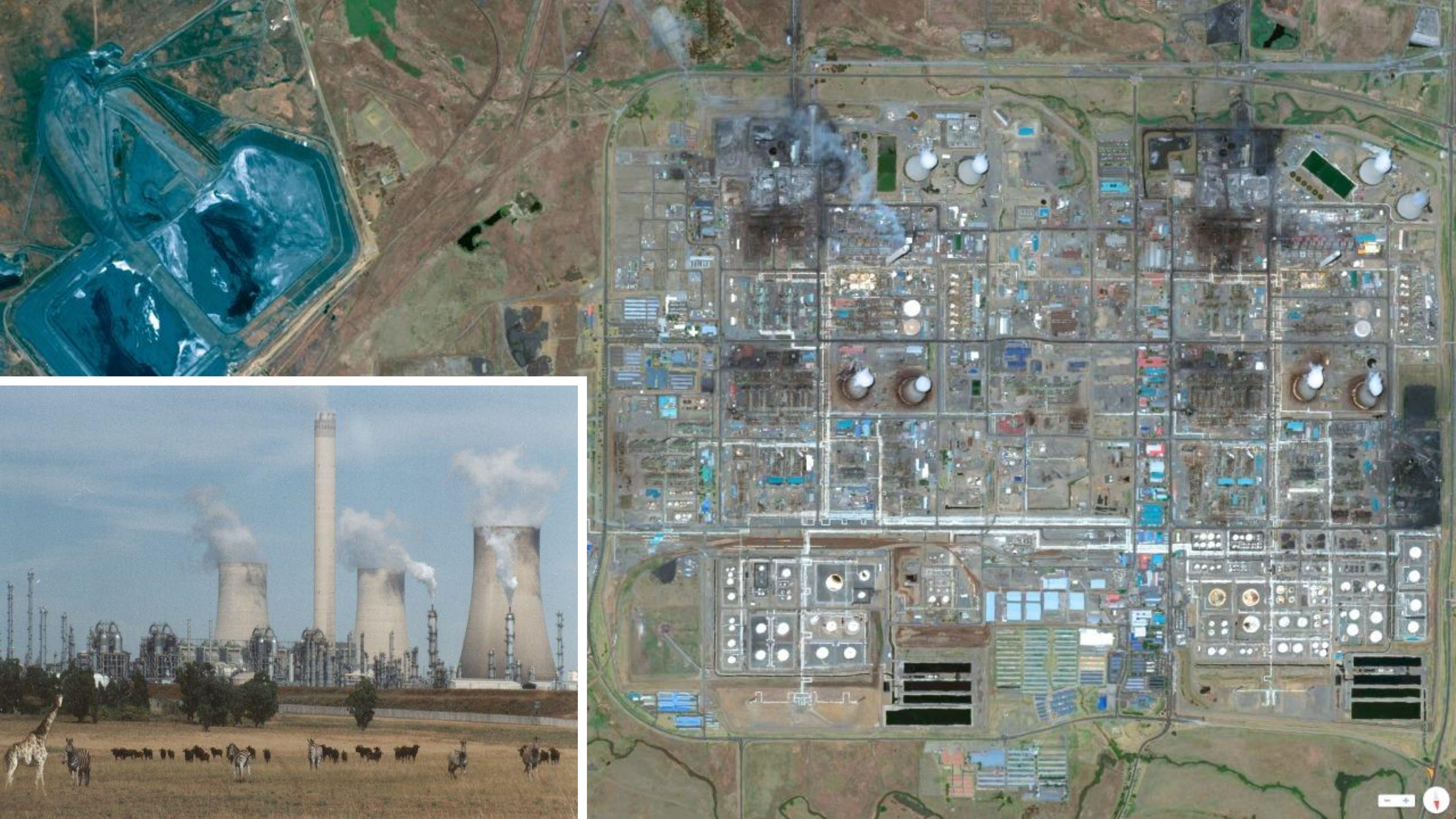
Continuous Process Industry Automation

Hierarchical, temporally decoupled control



My 4^{th}–65^{th} cyberphysical systems

Australia, Brazil, Britain, Canada, France, Germany, Hungary, India, Japan, Korea, Malaysia, Mexico, Singapore, South Africa, United States




zanini 20t
DEMAG
DEMAG


SAÍDA

Cyberphysical systems

	USA	Canada	Korea	South Africa	Australia	France	Germany	Hungary	Japan	Malaysia	Scotland	Brazil	**Grand Total**
Chemical Plant	12	4	1	1			1		1	1	1		**22**
Oil Refinery	12	3	1		1	1		1					**19**
Discrete Manufacturing Plant	9	1											**10**
Mine	3	2		1								1	**7**
Paper Mill		2											**2**
Power Plant	2												**2**
Aluminum Mill		1											**1**
Pipeline	1												**1**
Steel Mill		1											**1**
Grand Total	**39**	**14**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**65**

Feedback is amazing

The Power of Feedback

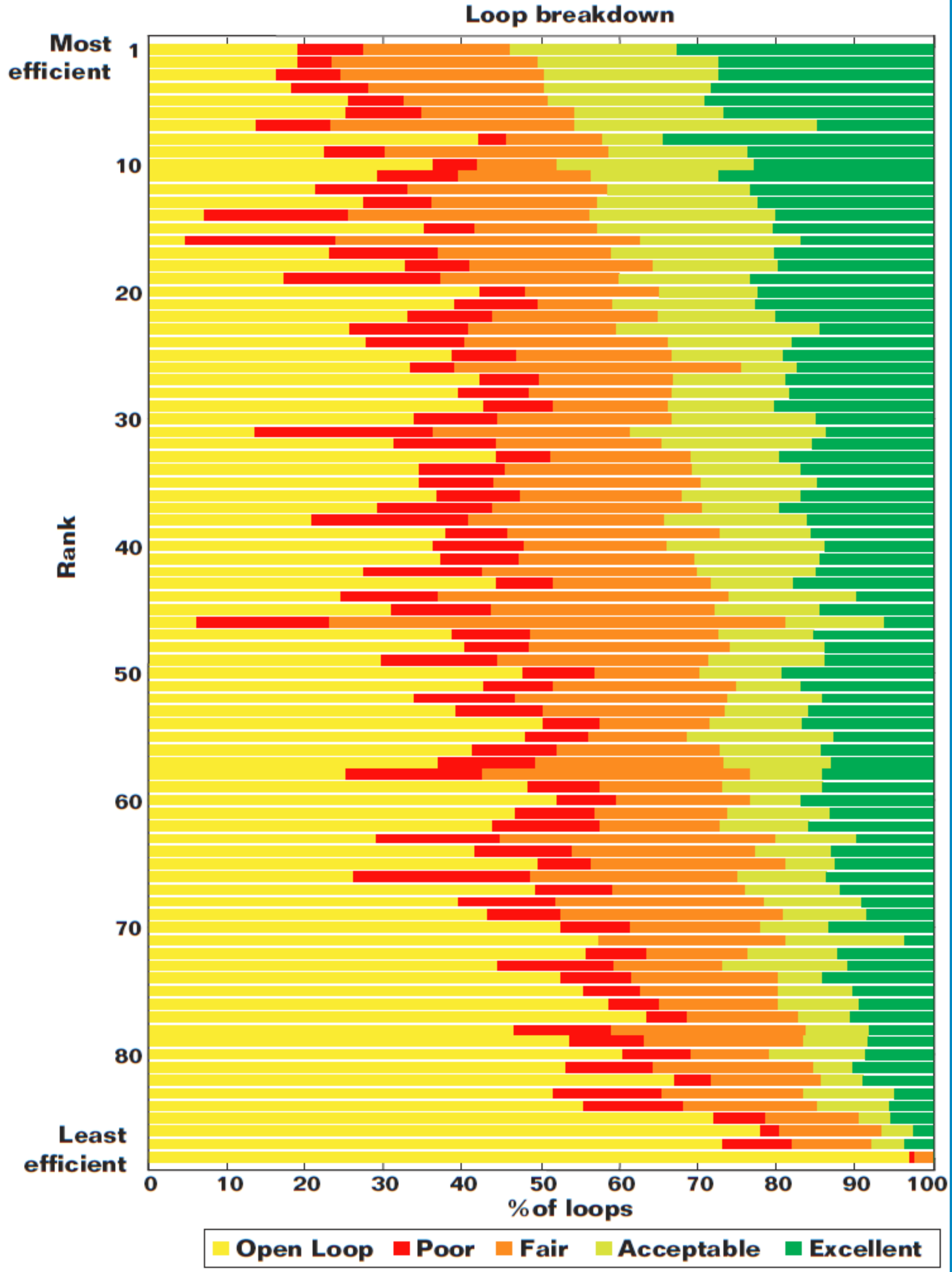
Karl Åström

Feedback has some amazing properties, it can

- make a system insensitive to disturbances and component variations,
- make good systems from bad components,
- stabilize an unstable system,
- create desired behavior, for example linear behavior from nonlinear components.

The major drawbacks are that

- feedback can cause instabilities
- sensor noise is fed into the system



It mostly works

- 1000 facilities, 250,000 loops
- Tuning, sticky valves, common oscilllations

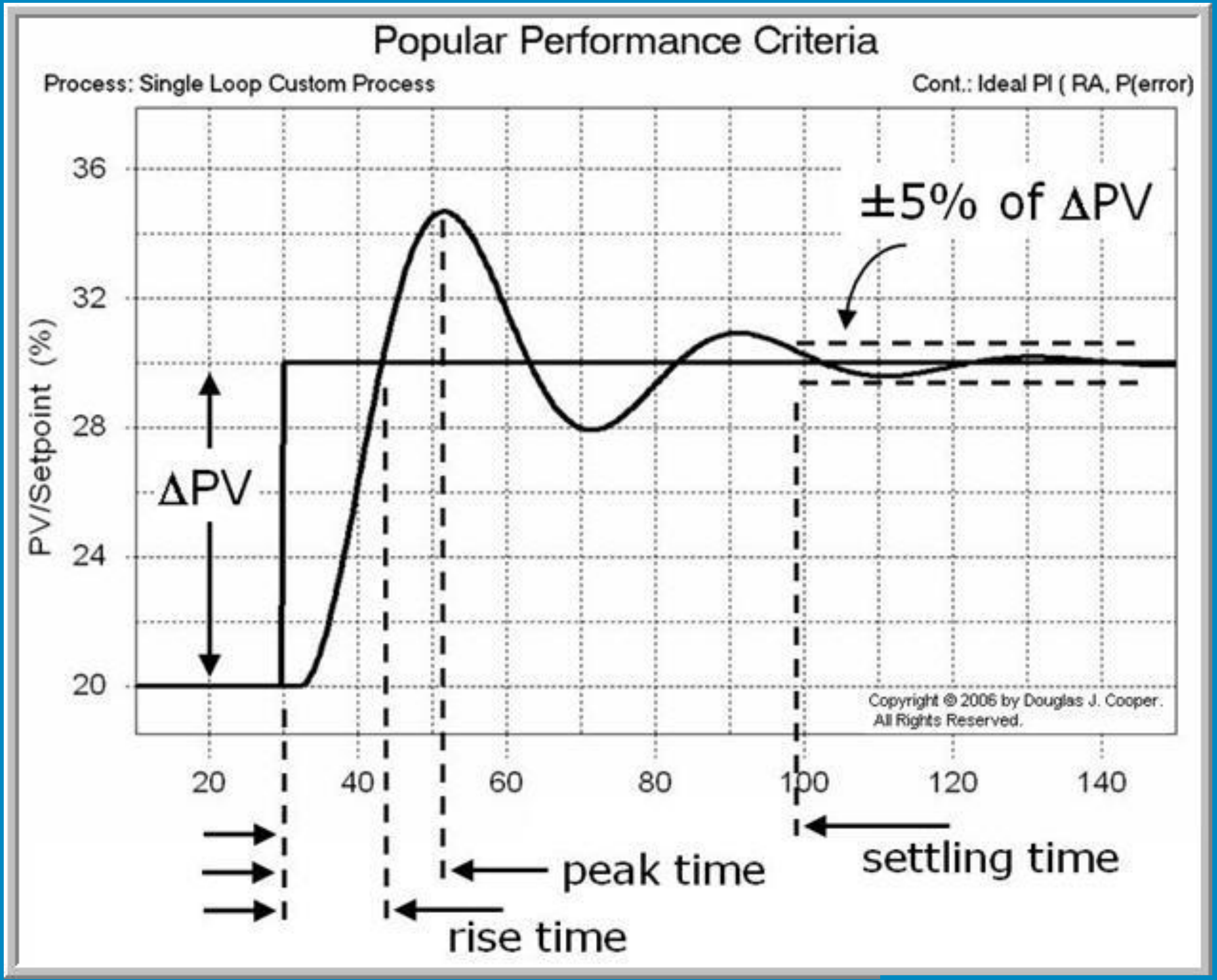
Desborough, Lane, Perry Nordh, and Randy Miller. "Process Out of Control.“ InTech - International Journal for Measurement Control 48.8 (2001): 52-56.

Desborough, Lane, and Randy Miller. "Increasing customer value of industrial control performance monitoring-Honeywell's experience." AIChE symposium series. American Institute of Chemical Engineers; 1998.

bigfoot BIOMEDICAL

Controller Performance

- Setpoint Response
- Cumulative Error
- Overshoot
- Harris Index*



* Desborough, Lane and Harris, Tom (1992). 'Performance assessment measures for univariate feedback control'. Canadian Journal of Chemical Engineering.

Why do we use feedback?

The purpose of control is to safely transfer variability from a place where it hurts (the controlled variable) to the place where it doesn't hurt as much (the manipulated variable) so that we don't have to do as much work

From: **To:**


Cruise control:



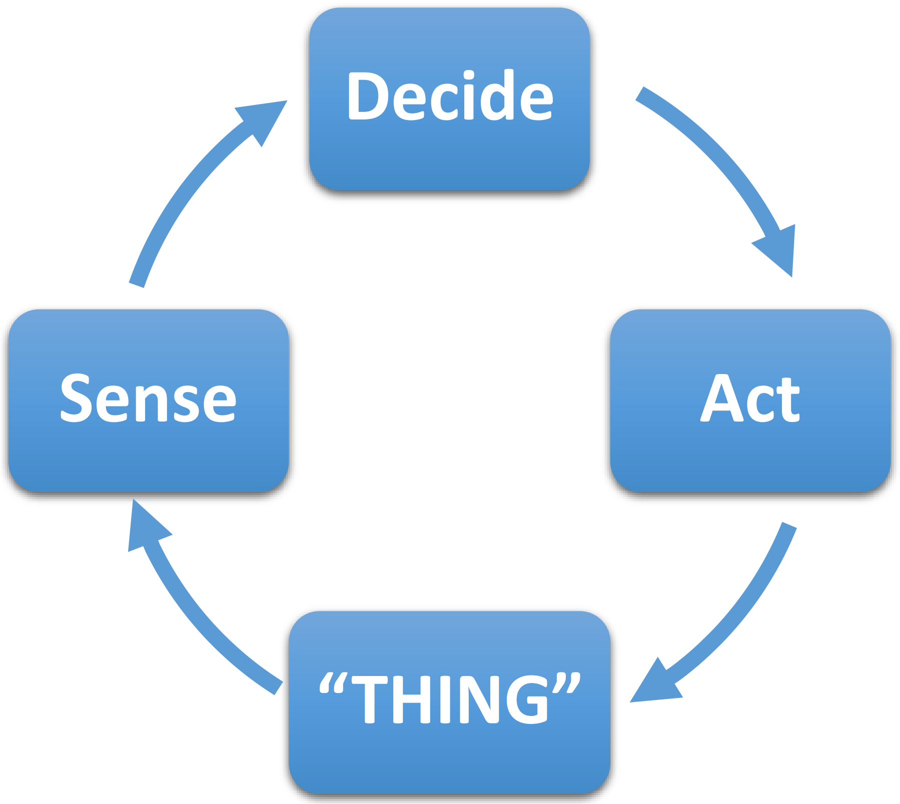
Thermostat:

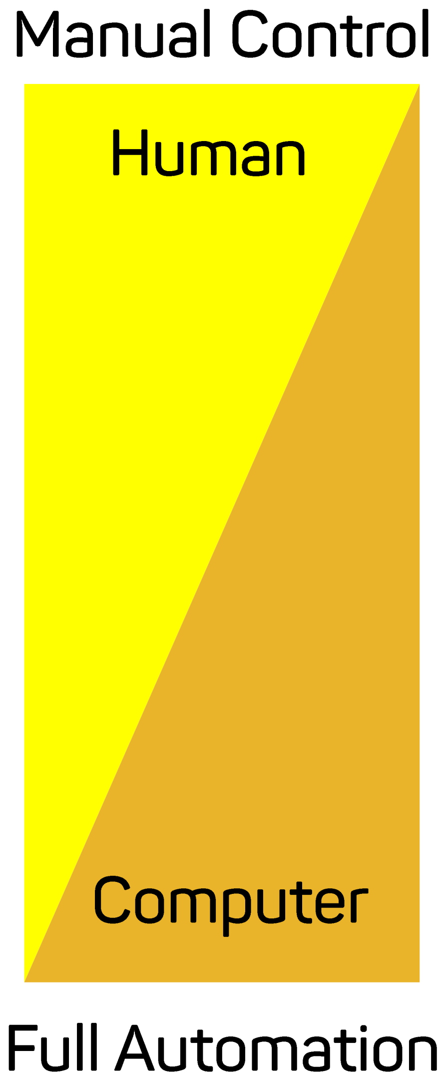


Control System:

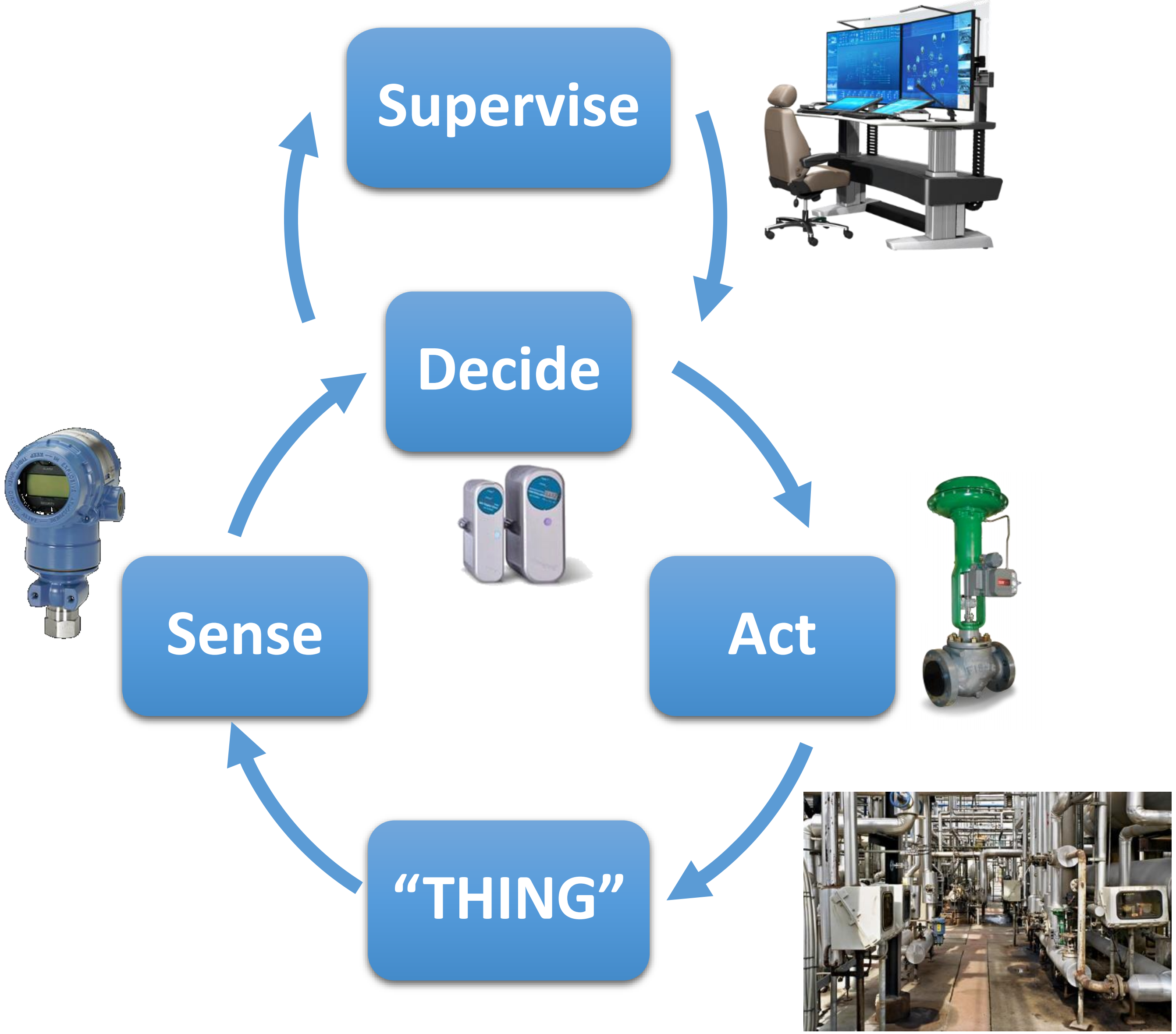

Autopilot

Opportunity: Feedback automates tasks





Automation adds new tasks



- Supervision
- Troubleshooting
- System maintenance


DON'T WAKE ME I'M WORKING


Don’t forget the human!


N1786B
N1786B
N1786B
N1786B

Humans and computers are good at different things

"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 automation may result in:

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

Automation is not a panacea

- Deskilling, Complacency, Addiction, Miscalibrated Trust

  Lack of practice can result in degradation of basic knowledge and skills

- Task Saturation, Brittleness, Mode Confusion, Loss of Situational Awareness

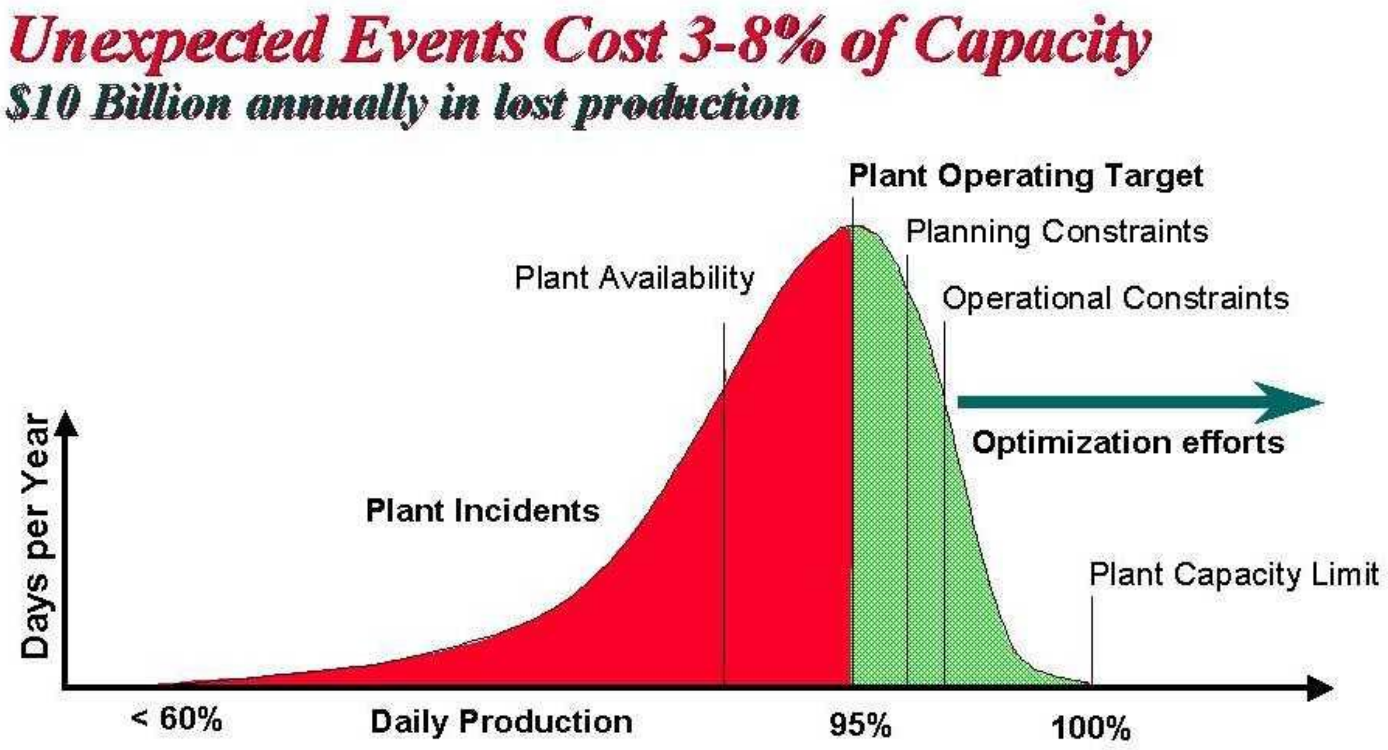
  Use of automated systems can reduce workload during normal operations but may add complexity and workload during demanding situations

Automation and Safety Forum 02, 03 June 2015 Brussels: Findings and Conclusions https://www.skybrary.aero/bookshelf/books/3105.pdf
Nancy Leveson, “Engineering a Safer World”; American Airlines, “Children of the Magenta”; David Mindell, “Our Robots, Ourselves”; Some Lessons Learned About Flight Deck Automated Systems, Kathy Abbott, PhD, FRAeS Federal Aviation Administration 2 June 2015, https://www.skybrary.aero/bookshelf/books/3094.pdf; Levels of Automation Advantages & Disadvantages, https://www.skybrary.aero/bookshelf/books/3120.pdf

Abnormal Situation Management®

Joint Research and Development Consortium

Honeywell
ConocoPhillips
USER CENTERED DESIGN SERVICES
Achieving Excellence in Control Room Operations
ExxonMobil
Celanese
TTS
UCLA
ChevronTexaco
BAW Architecture
Shell
NOVA Chemicals®

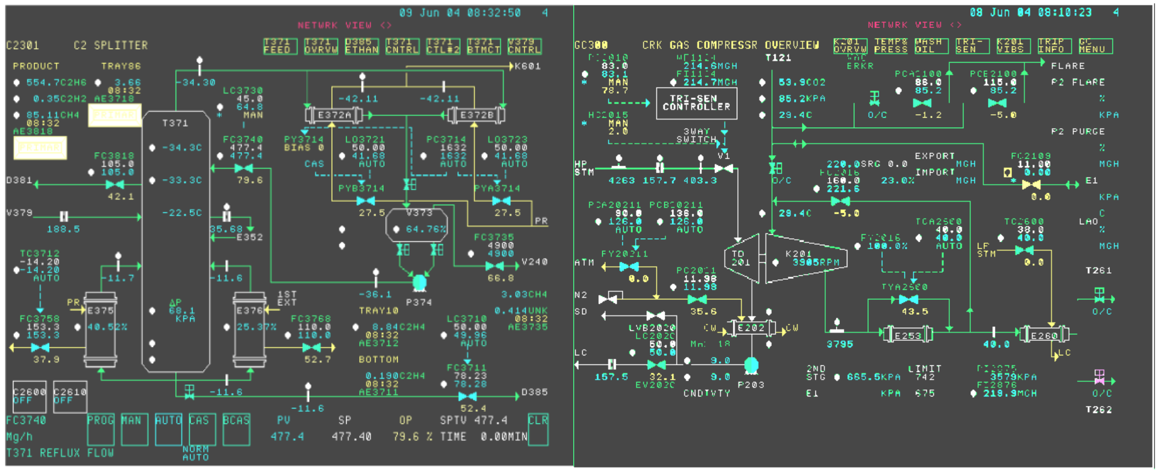


www.asmconsortium.com

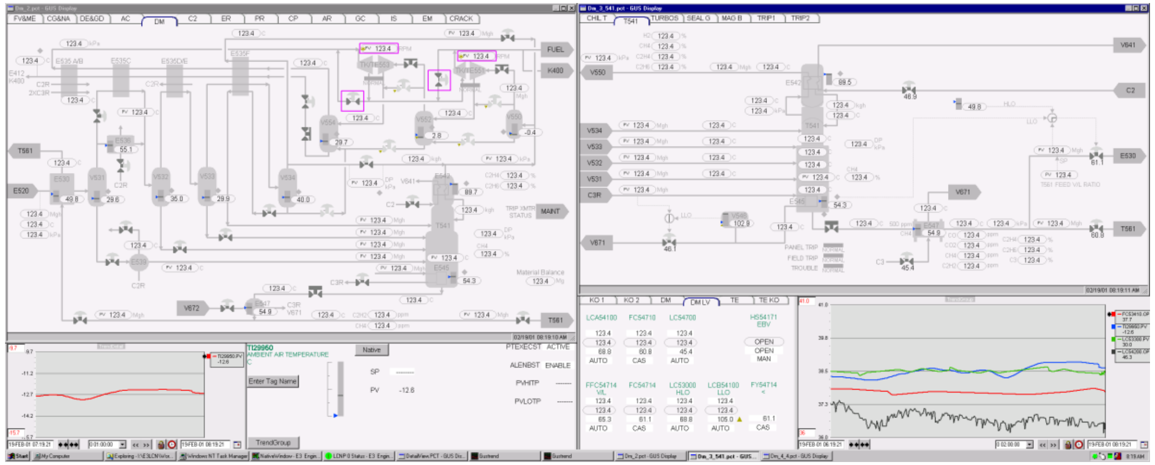
ASM

Human Factors and Automation

Effective visual workplaces help “make problems visible”



vs.



Operator displays make a huge difference:

Responded faster and more consistently to abnormal situations

- 35%-48% improvement over the traditional console

Recognized, before the first alarm, that an abnormal situation was present in 48% of the situations

- 38% improvement over the traditional console

Successfully dealt with 96% of the abnormal situations

- 26% improvement over the traditional console

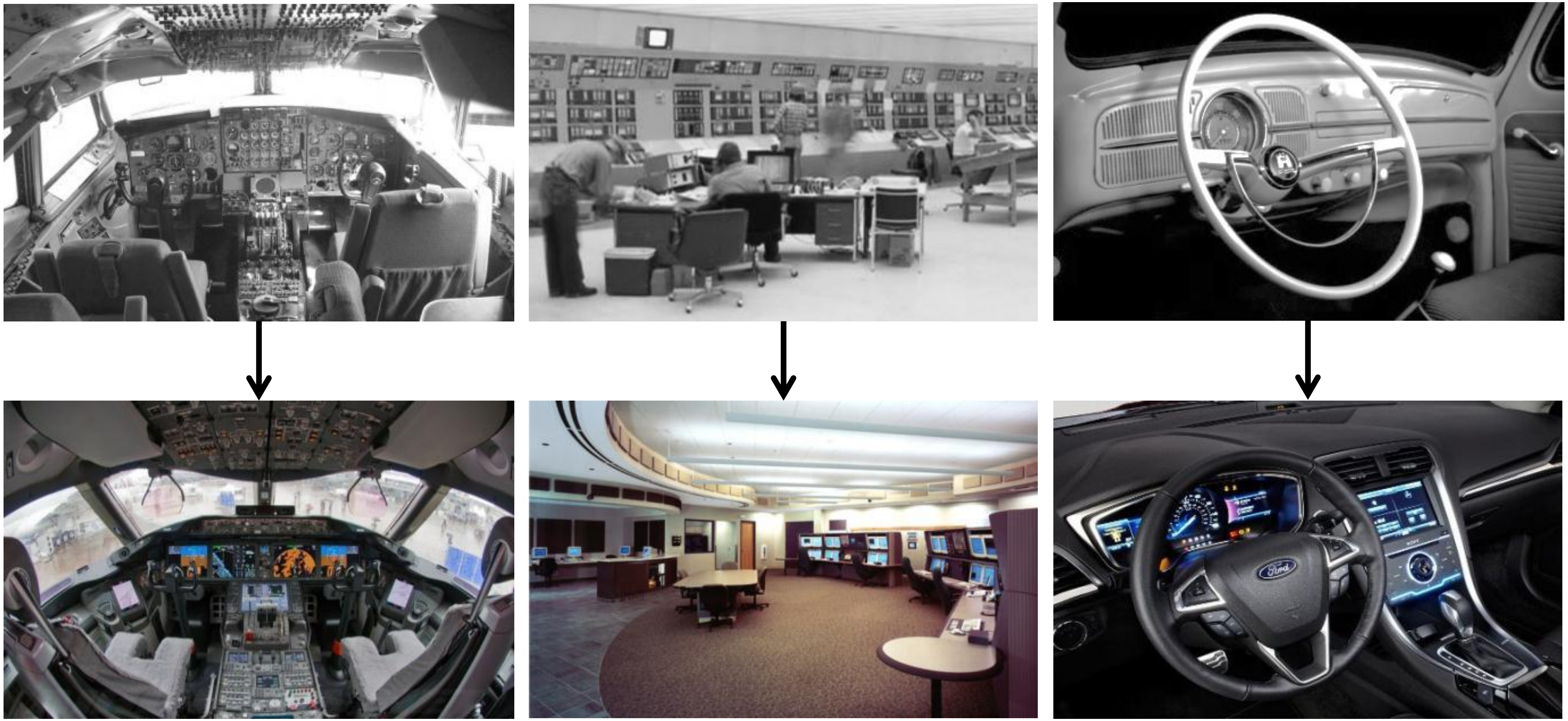
<u>Source</u>: Errington, DeMaere, and Wade “Supporting Key Console Operator Interactions through the Control System Interface”, 2005 AIChE meeting.

Human Centered Automation

Situational Awareness / Appropriate Automation / Usability Principles

Old

New



My most recent cyberphysical system

Insulin requiring diabetes has a large unmet need

A **data driven** disease

where an **average person** is required to **self-titrate**

a **dangerous medicine** on a **24x7x365** basis;

more than **66%** of them

are treated by **primary care physicians**

Insulin delivery is crushingly burdensome

- Physical Burden
  - extra devices on the body
  - needles, catheters, sensors, and finger sticks
  - sleep deprivation
  - food, exercise, travel limitations
  - chronic complications (retinopathy, neuropathy, nephropathy)
- Financial Burden
  - short term costs, long term costs
  - sick days
  - opportunity costs
  - indirect costs
- Cognitive Burden
  - observation tasks
  - calculations
  - problem solving tasks
  - therapy management tasks
  - skill development and retention tasks
  - supply management tasks
- Emotional Burden
  - fear of hypos
  - fear of chronic complications
  - self-image, depression, self-esteem

30 years of industrial automation experience

- 1987 SCADA (Supervisory Control and Data Acquisition)
- 1989 PID (Proportional Integral Derivative)
- 1993 MPC (Model Predictive Control)
- 1994 ASM (Abnormal Situation Management)
- 1998 CPM (Controller Performance Assessment)
- 1999 Industrial Automation Systems
- 2003 Agile Software Development
- 2004 Lean Product Development
- 2006 System Safety Engineering
- 2008 Remote Monitoring and Diagnostics
- 2010 Medical Device Engineering
- 2011 MBD (Model-Based Design)
- 2014 Modeling and Simulation
- 2016 Direct to Code
- 2017 Statistics

UNIVERSITY OF WATERLOO

Queen's UNIVERSITY

NOVA Chemicals

Honeywell Process Solutions

GE Energy

Medtronic For People with Diabetes

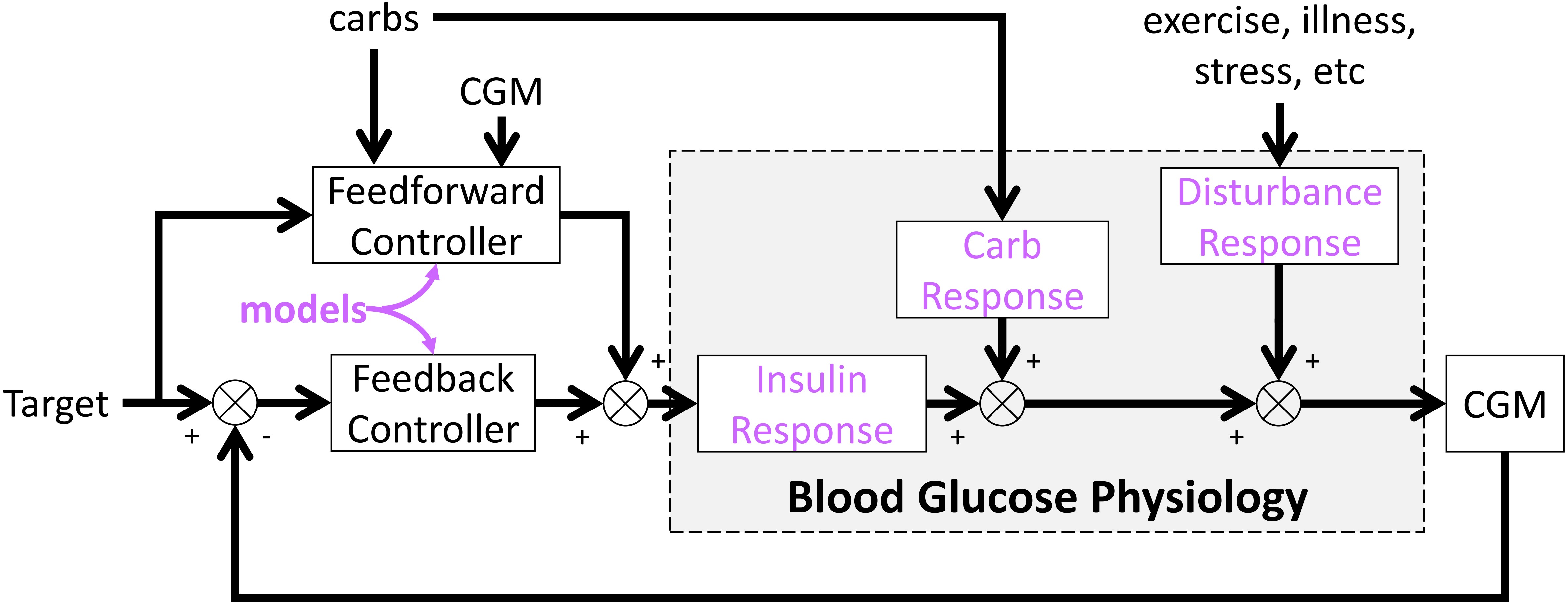
bigfoot BIOMEDICAL


bigfoot
BIOMEDICAL

Bigfoot Loop Investigational System

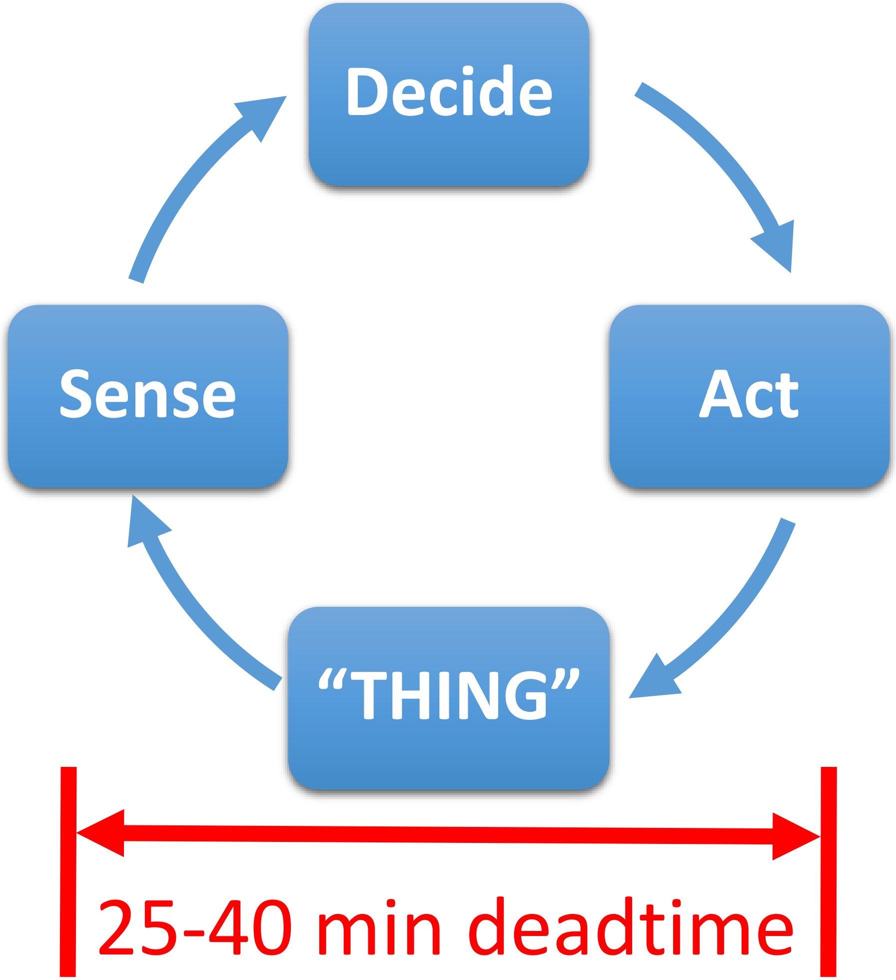
CAUTION - Investigational Device. Limited by Federal (or United States) law to investigational use.

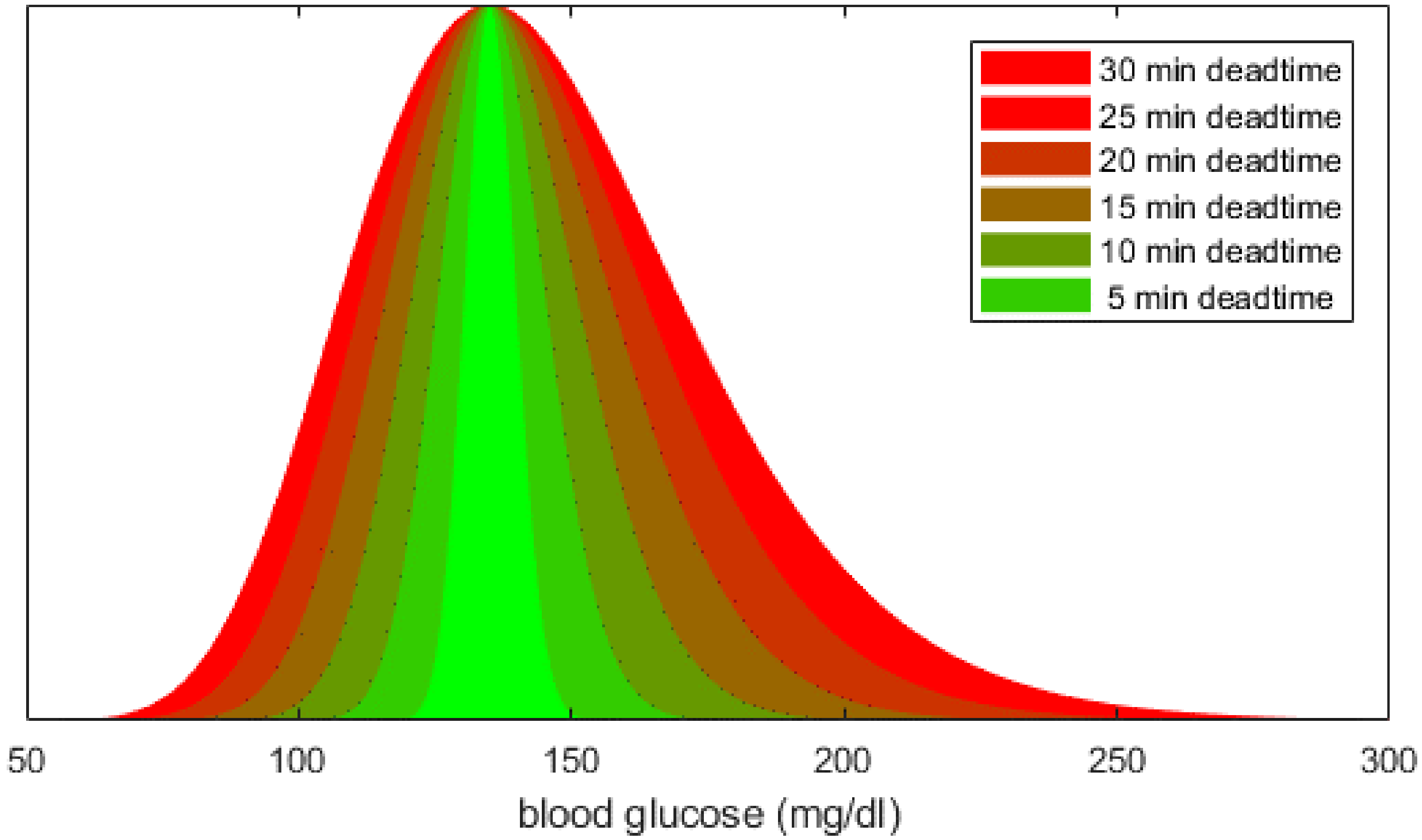
Automated Insulin Delivery



Challenges

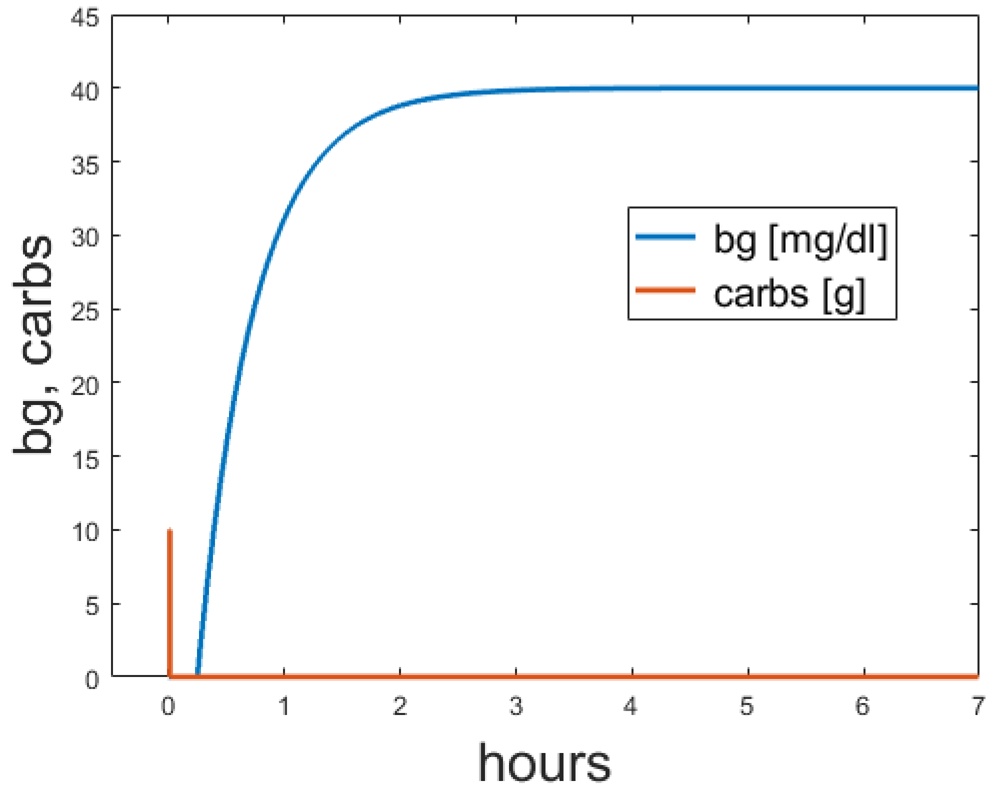
Deadtime limits the amount of variability transfer



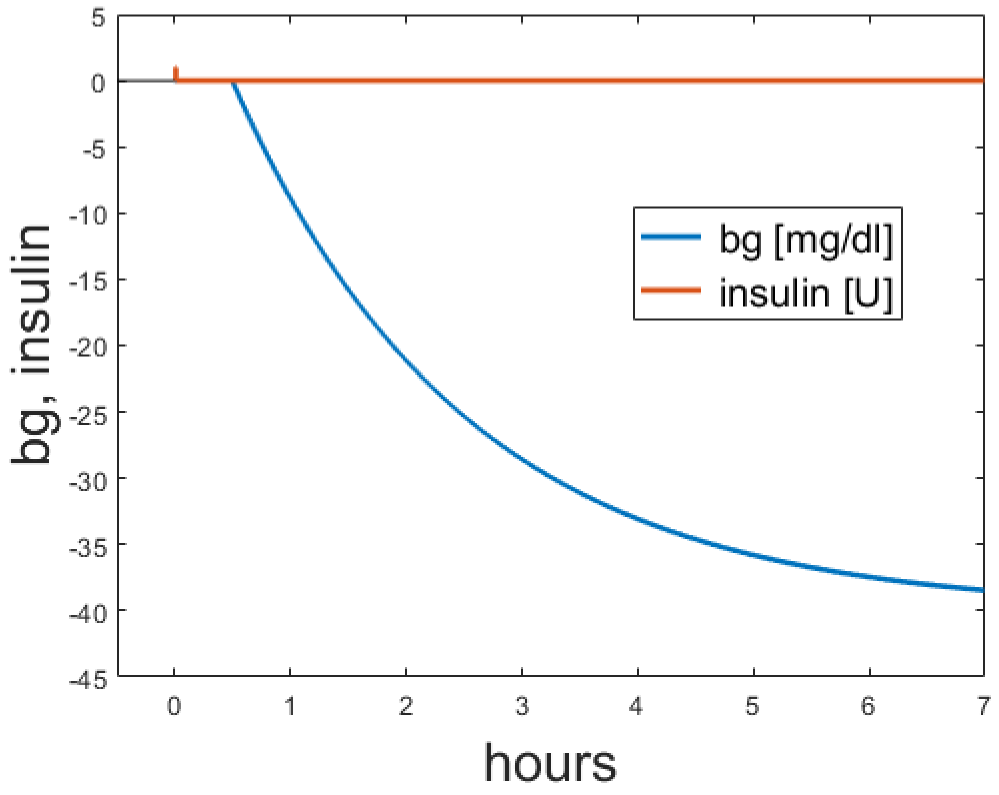


Dynamic Models / Transfer Functions

Carbohydrate Response

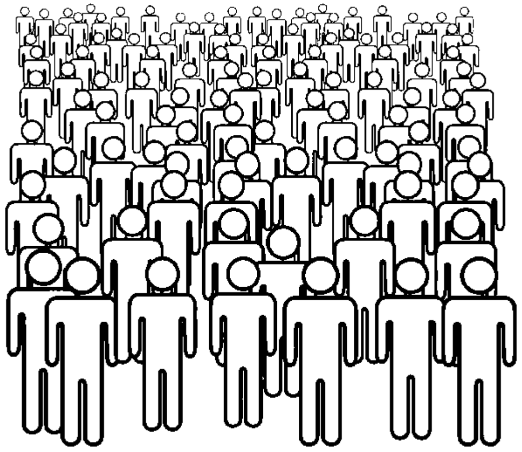


Insulin Response



Our system needs to work across a wide range of users and use conditions

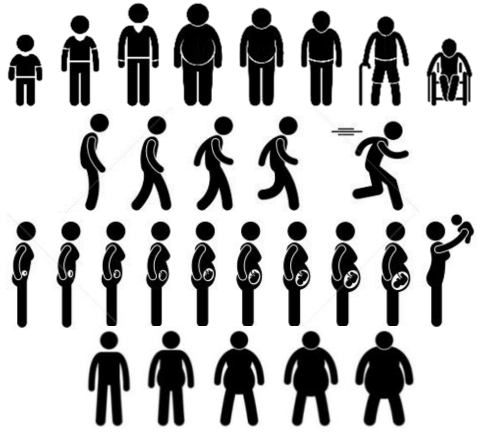
change
across
population



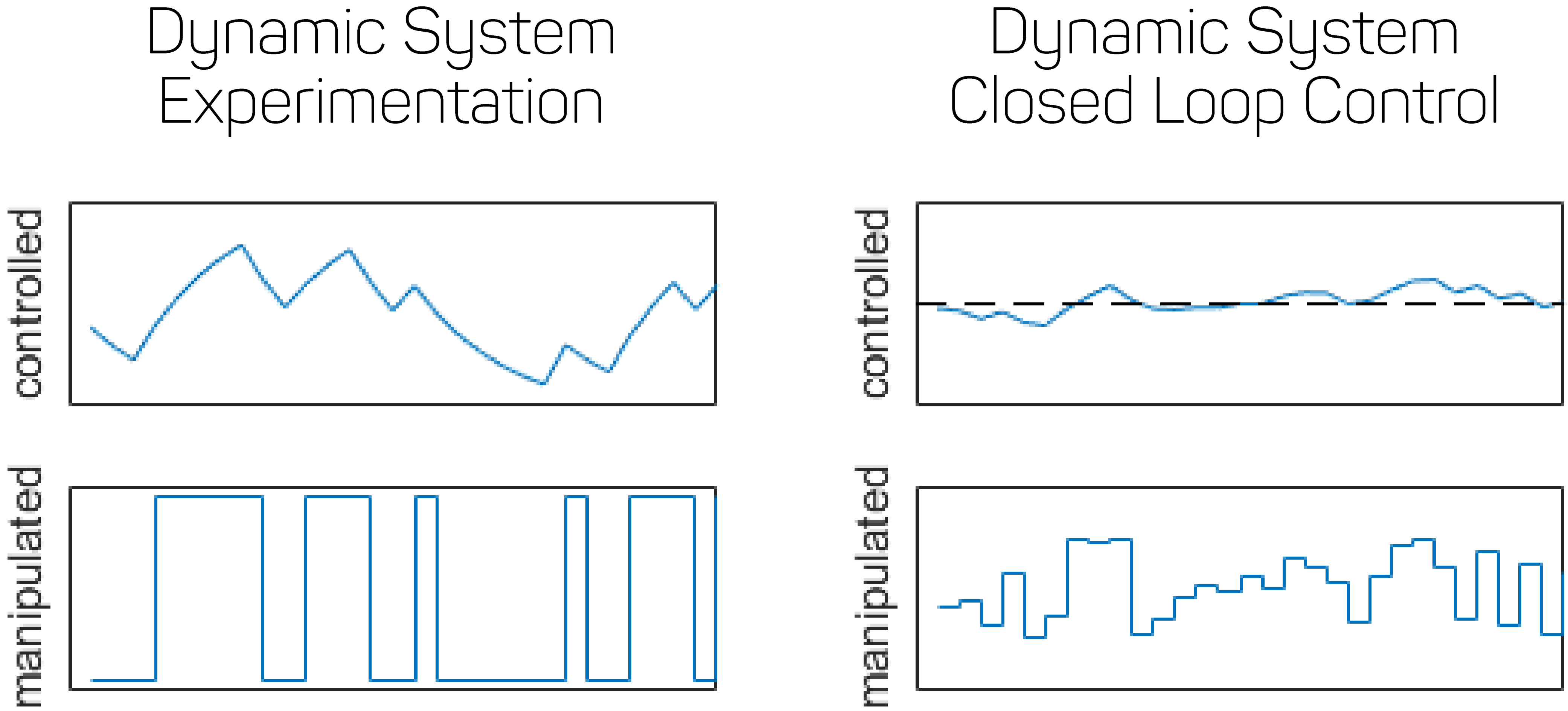
change
throughout
the day

change
with activities
and events

change
over
time



Experimentation is slow, difficult, and dangerous



Experimentation is slow, difficult, and dangerous

non-Gaussian distributions
lack of persistent excitation
short sample lengths
time consuming
unmeasured inputs
unrealistic
inconsistent recording
small datasets
nonlinearities
poor repeatability
sensor artifacts
varying dynamics
patient risk
coincident inputs
expensive
missing data
inaccurate sensing

Temporal constraints

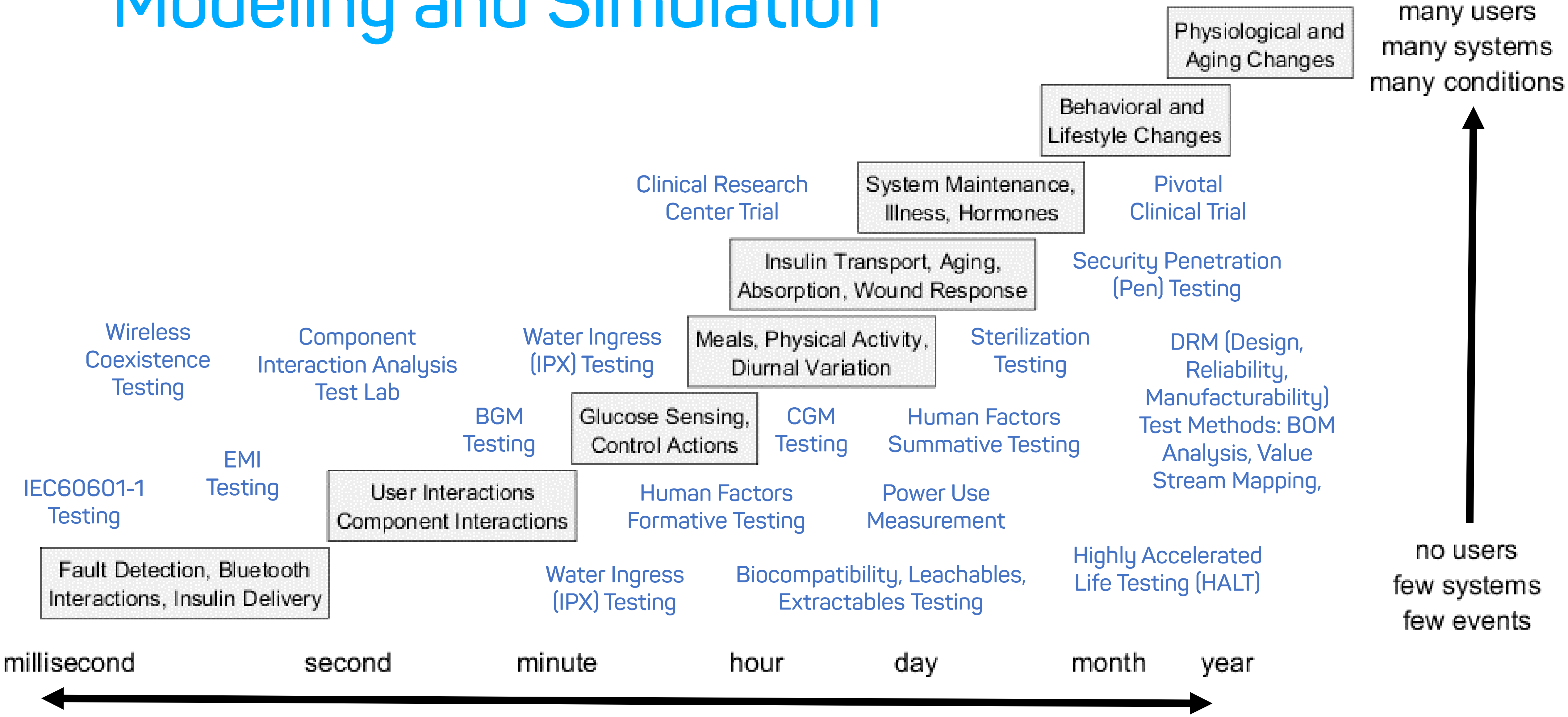
- There should not be prolonged periods of low blood glucose caused by overdelivery of insulin, which can lead to coma and death
- There should not be prolonged periods of complete absence of insulin, which can lead to DKA (diabetic ketoacidosis), high blood glucose, and death

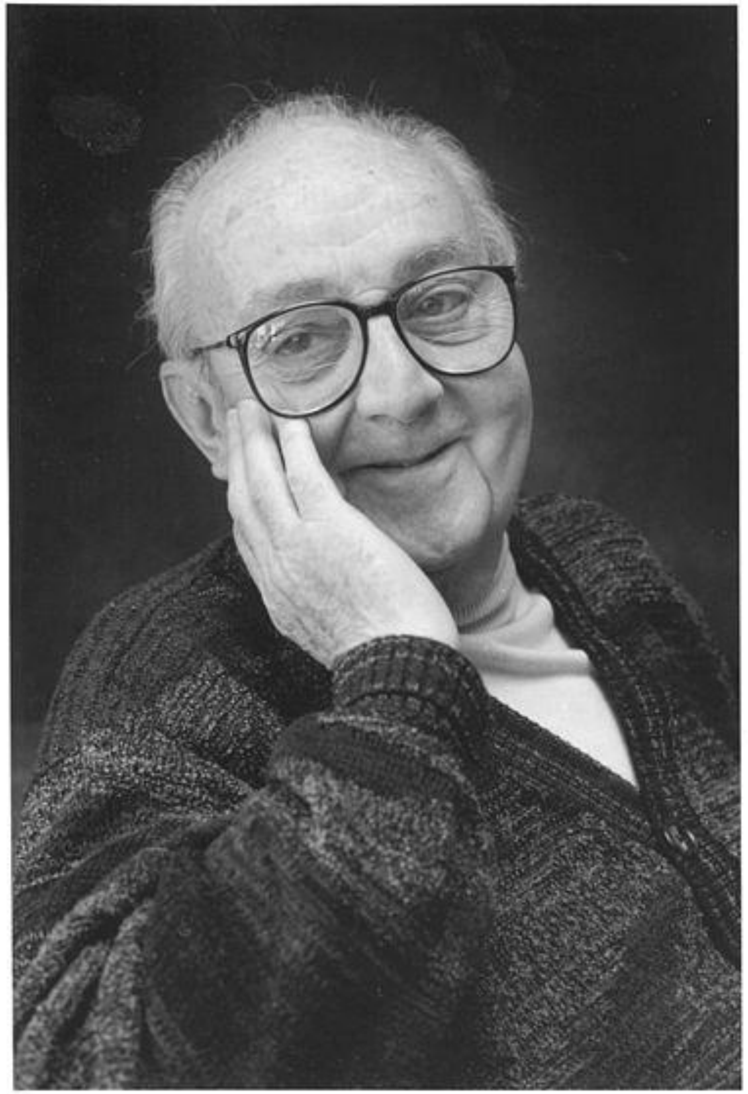
Modeling and Simulation to the rescue

Models enable us to efficiently characterize what the system will do

Model (noun):
A simplified representation used to explain the workings of a real world system or event.

Modeling and Simulation





"All models are wrong,
but some are useful"

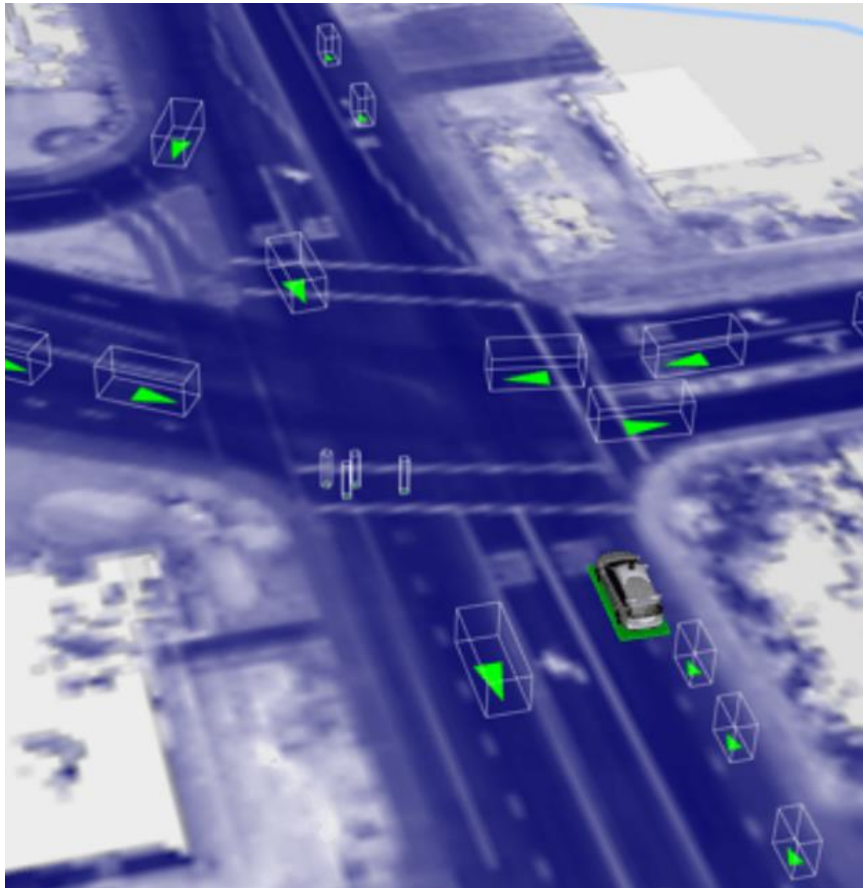
\- George Box

Modeling gotchas

- Purpose
  - Explanation vs. Prediction
  - Open- vs. Closed-loop
- Implementation
  - Overfitting
  - Unnecessary Complexity
- Don't forget
  - Stoichasticity
  - Sensitivity analysis
  - Verification and validation

1. Law, Averill M., W. David Kelton, and W. David Kelton. *Simulation modeling and analysis*. Vol. 3. New York: McGraw-Hill, 2007.
2. Shmueli, Galit. "To explain or to predict?." *Statistical science*(2010): 289-310.
3. Saltelli, A., Tarantola, S., Campolongo, F., and Ratto, M. (2004). Sensitivity Analysis in Practice - A Guide to Assessing Scientific Models. Wiley.
4. MacGregor, John F., Thomas J. Harris, and J. D. Wright. "Duality between the control of processes subject to randomly occurring deterministic disturbances and ARIMA stochastic disturbances." *Technometrics* 26.4 (1984): 389-397.
5. Sterman, John D. "A skeptic's guide to computer models." *Managing a nation: The microcomputer software catalog* 2 (1991): 209-229.
6. Sargent, Robert G. "Verification and validation of simulation models."*Simulation Conference (WSC), Proceedings of the 2010 Winter*. IEEE, 2010.
7. Hjalmarsson, H. (2005). From experiment design to closed-loop control. Automatica, 41(3), 393-438.
8. Roy, C. J., & Oberkampf, W. L. (2011). A comprehensive framework for verification, validation, and uncertainty quantification in scientific computing. Computer methods in applied mechanics and engineering, 200(25), 2131-2144.
9. Pianosi, F., Beven, K., Freer, J., Hall, J. W., Rougier, J., Stephenson, D. B., & Wagener, T. (2016). Sensitivity analysis of environmental models: A systematic review with practical workflow. Environmental Modelling & Software, 79, 214-232.

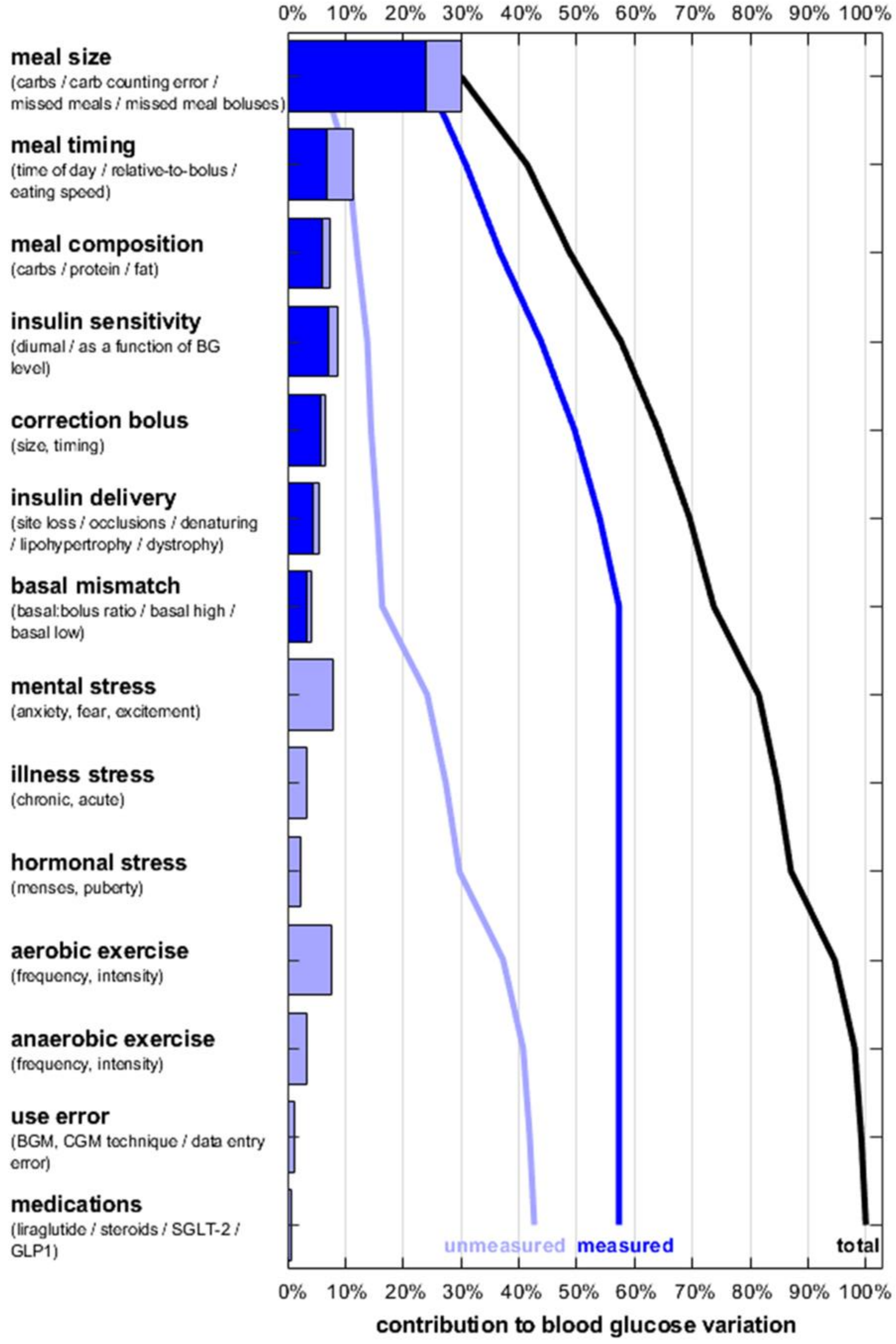
Modeling and Simulation



Alexis C. Madrigal, "Inside Waymo's Secret World for Training Self-Driving Cars", The Atlantic, Aug 23, 2017

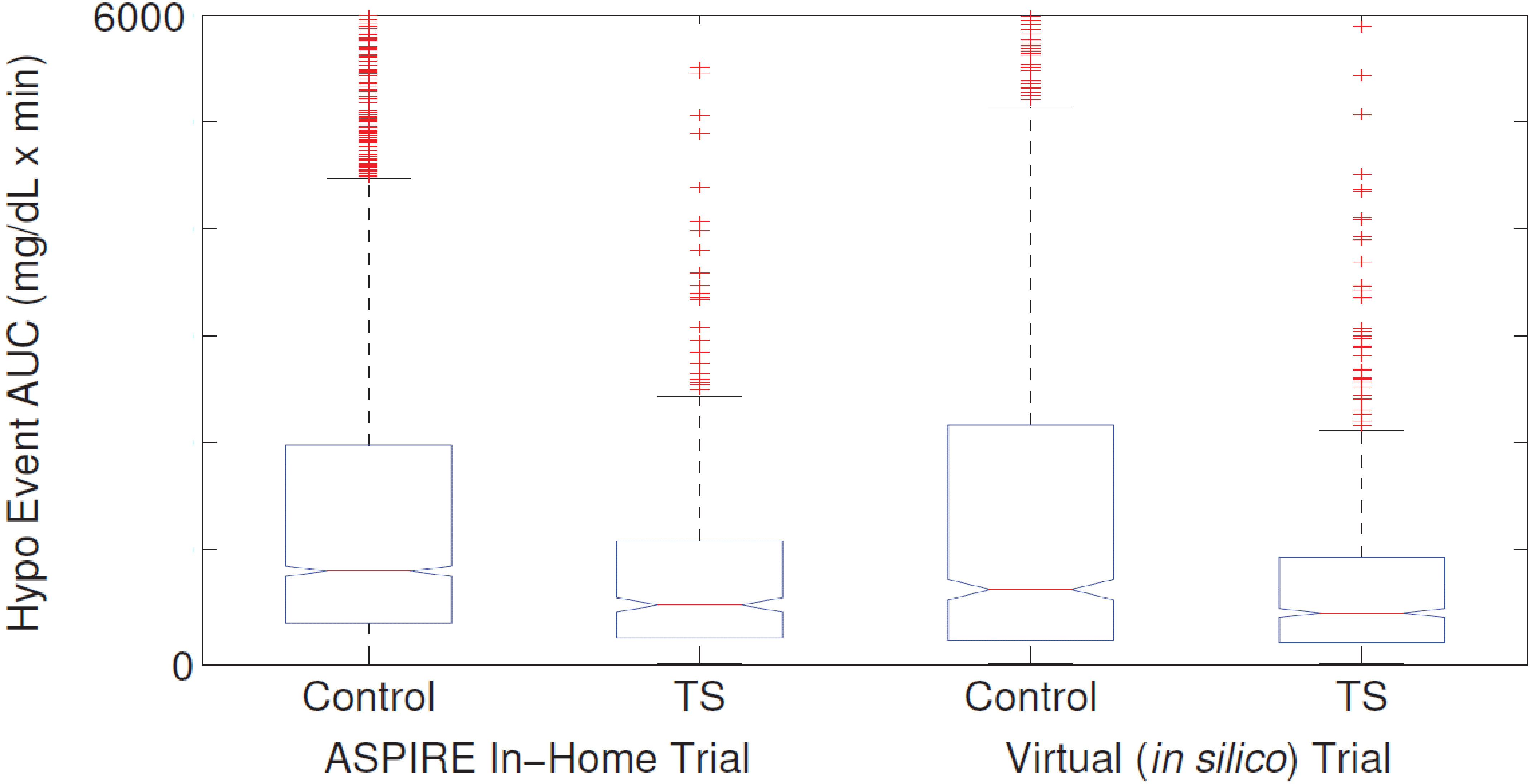
- Variance reduction techniques
- Monte Carlo simulation
- Population sampling
- Complex and challenging scenarios
  - Simultaneous faults
  - Risky behaviors
  - Challenging responses

Michael DeKort, "Autonomous Levels 4 and 5 will never be reached without Simulation", June 20, 2017



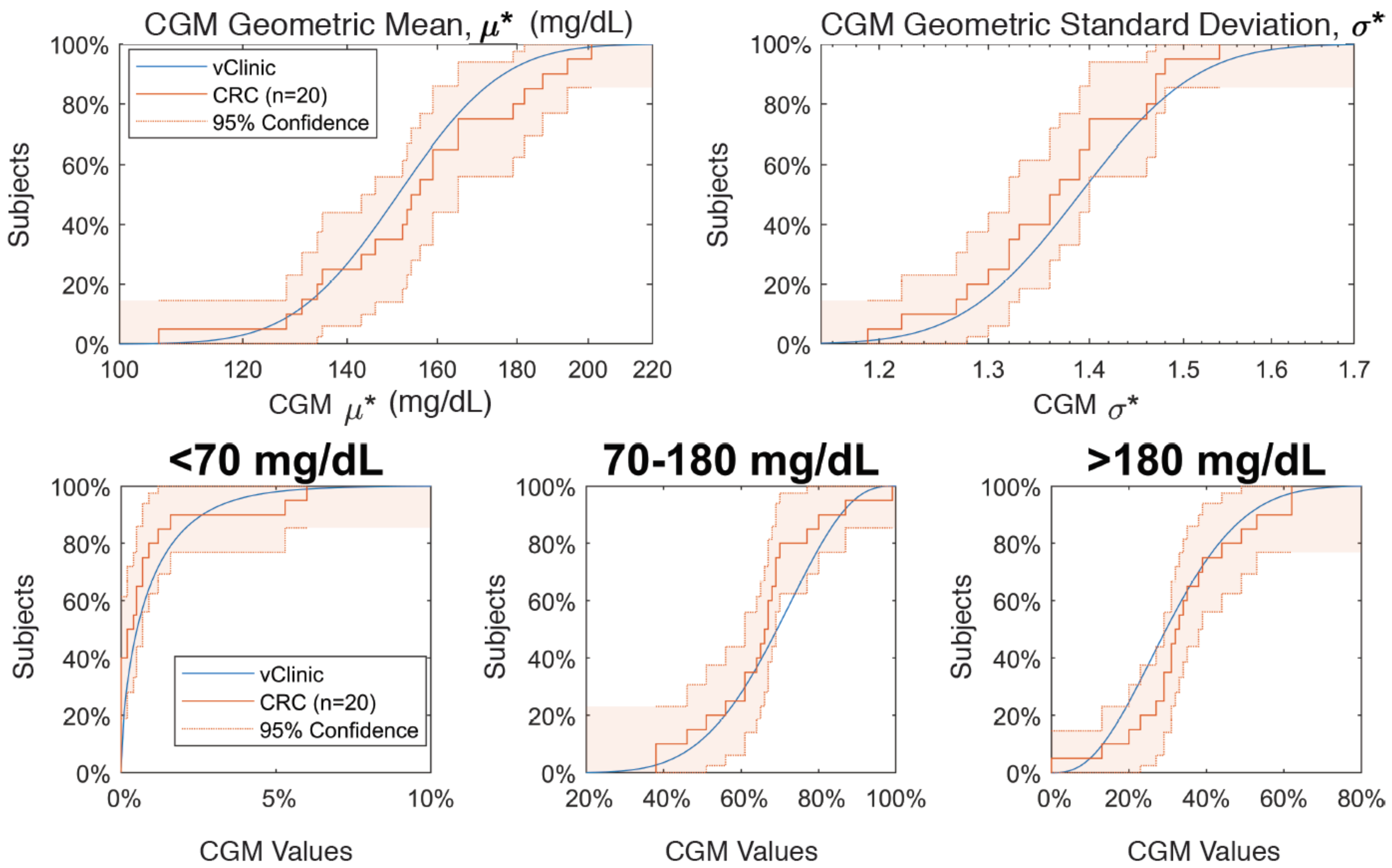
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
meal size
(carbs / carb counting error / missed meals / missed meal boluses)
meal timing
(time of day / relative-to-bolus / eating speed)
meal composition
(carbs / protein / fat)
insulin sensitivity
(diurnal / as a function of BG level)
correction bolus
(size, timing)
insulin delivery
(site loss / occlusions / denaturing / lipohypertrophy / dystrophy)
basal mismatch
(basal:bolus ratio / basal high / basal low)
mental stress
(anxiety, fear, excitement)
illness stress
(chronic, acute)
hormonal stress
(menses, puberty)
aerobic exercise
(frequency, intensity)
anaerobic exercise
(frequency, intensity)
use error
(BGM, CGM technique / data entry error)
medications
(liraglutide / steroids / SGLT-2 / GLP1)
unmeasured
measured
total
contribution to blood glucose variation

Modeling and Simulation



Palerm, C. C., Lintereur, L., Monirabbasi, S., & Desborough, L. (2014, February). Virtual Trial Predicts Clinical Trial Outcomes-accelerating Development and Reducing Risk Through Model-based Design. Poster, ATTD 2014, Vienna, Austria.

Modeling and Simulation



Desborough, L, Naylor, R, Block, J, Buckingham, B, Pinsker, J, Wadwa, P, Forlenza, G, O'Brien, R, Lum, J, and B. Mazlish, "Leveraging Modeling and Simulation in the Development of the Bigfoot Biomedical Automated Insulin Delivery System", Poster, DTM 2017, Bethesda, MD.

Modeling and Simulation

With Modeling and Simulation:

- Rapidly evaluate multiple algorithm candidates and parameters
- Simulate performance of closed loop algorithms in a larger more varied population
- Inform design of clinical trial protocols, predict outcomes
- Predict performance over months or years of use

Modeling and Simulation

With Modeling and Simulation:

- Rapidly evaluate multiple algorithm candidates and parameters
- Simulate performance of closed loop algorithms in a larger more varied population
- Inform design of clinical trial protocols, predict outcomes
- Predict performance over months or years of use

Plus:

- Perform experiments in ways not possible or safe to do in in-vivo clinical trials
- No IRB or exclusion criteria are necessary
- No recruitment bias

Modeling and Simulation

With Modeling and Simulation:

- Rapidly evaluate multiple algorithm candidates and parameters
- Simulate performance of closed loop algorithms in a larger more varied population
- Inform design of clinical trial protocols, predict outcomes
- Predict performance over months or years of use

Plus:

- Perform experiments in ways not possible or safe to do in in-vivo clinical trials
- No IRB or exclusion criteria are necessary
- No recruitment bias
- 4,000,000 times faster and less expensive than real-time (~1 cent per simulated contact-day vs. ~$1,500 per contact-hour)

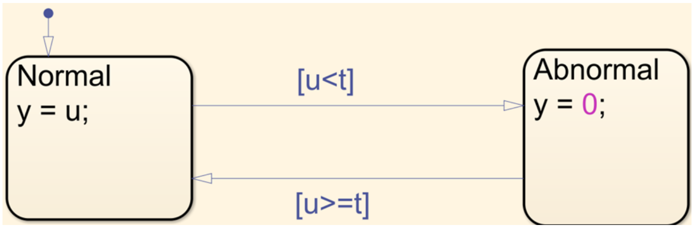
Model Based Design

- Model and simulate algorithms and entire systems
- Automatically generate C code
- Verify and validate the design

https://www.mathworks.com/solutions/medical-devices.html

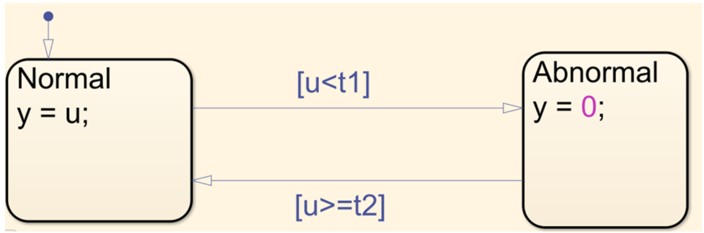
As the problem gets more complex, the code gets *really* complex

simple state machine



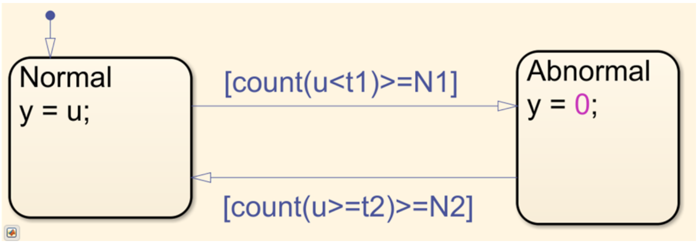

```
for i=1:length(inData)
    if(inData(i)>=t)
        outData(i) = inData(i);
    else
        outData(i) = 0;
    end
end
```

+ hysteresis




```
inNormalRegion = true;
for i=1:length(inData)
    if(inNormalRegion && (inData(i)<t1))
        inNormalRegion = false;
    elseif(~inNormalRegion && (inData(i)>=t2))
        inNormalRegion = true;
    end
    if(inNormalRegion)
        outData(i) = inData(i);
    else
        outData(i) = 0;
    end
end
```

+ hysteresis + debouncing



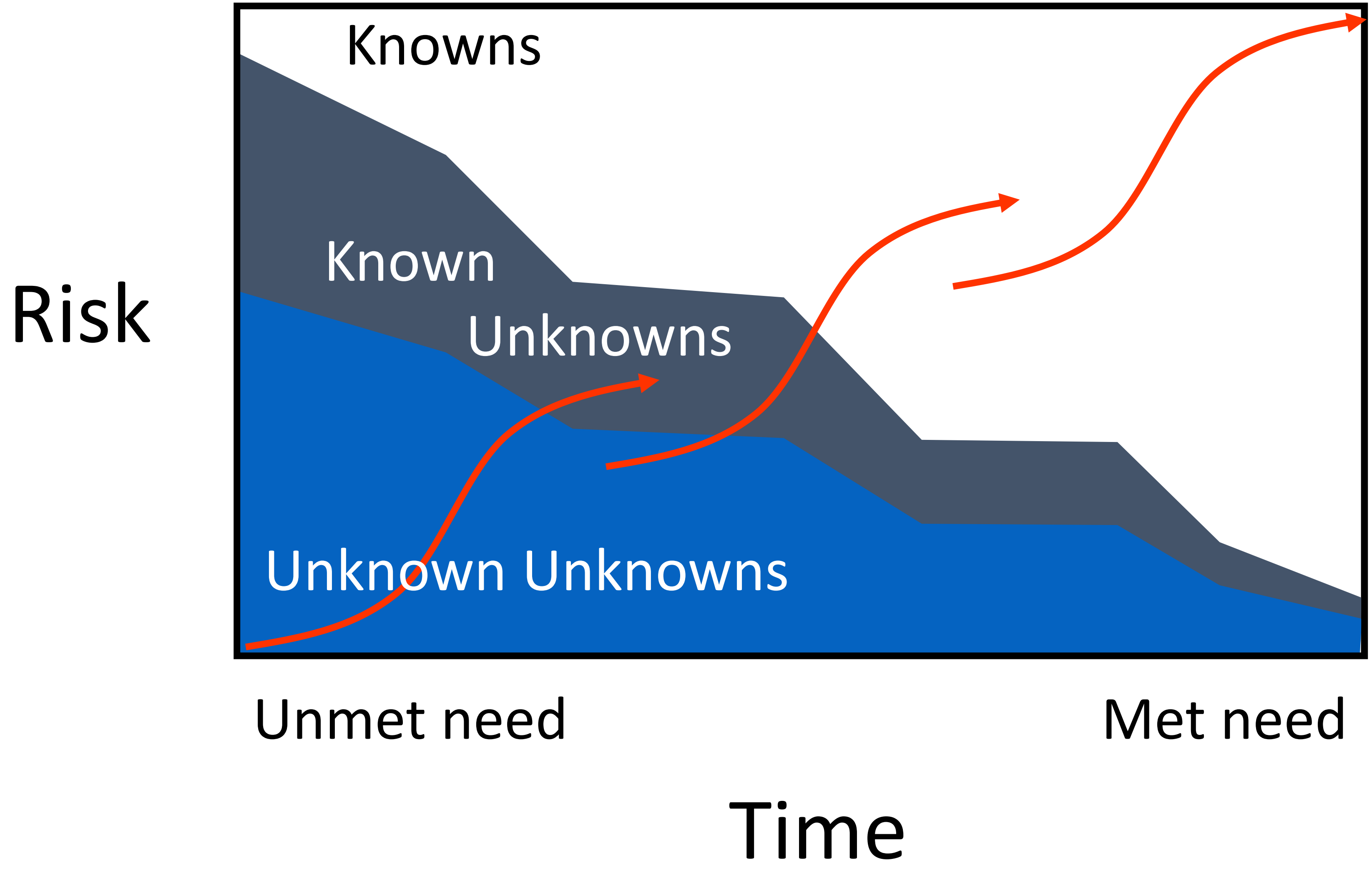

```
inNormalRegion = true;counter = 0;
for i=1:length(inData)
    if(inNormalRegion)
        if(inData(i)<t1)
            counter = counter+1;
            if(counter>=N1)
                inNormalRegion = false;
            end
        else;counter = 0;end
     else
        if(inData(i)>=t2)
            counter = counter+1;
            if(counter>=N2)
                inNormalRegion = true;
            end
        else; counter = 0; end
     end
     if(inNormalRegion)
         outData(i) = inData(i);
    else; outData(i) = 0; end
end
```

Model-Based Design

Ford
Honeywell
Dexcom®
Lexus
Toyota
Medtronic
Airbus
BMW
Caterpillar®
Tesla
Boeing
John Deere
Lockheed Martin

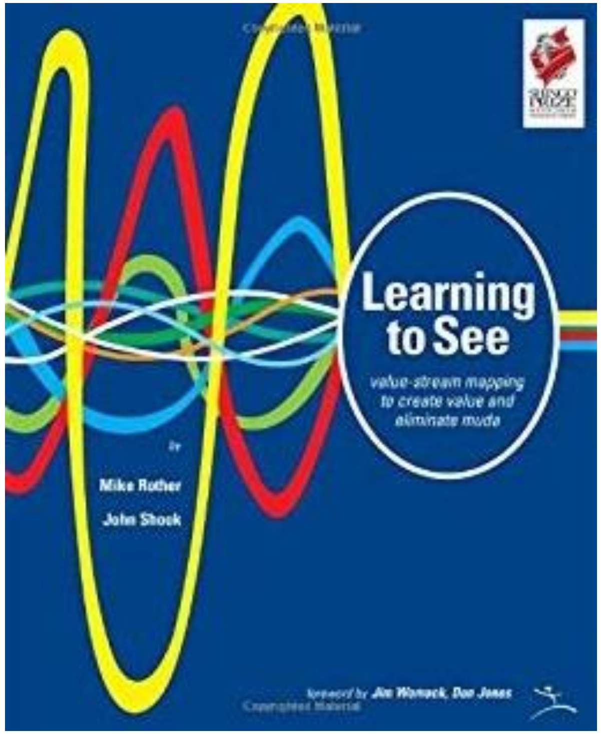
Complexity, variation, emergence

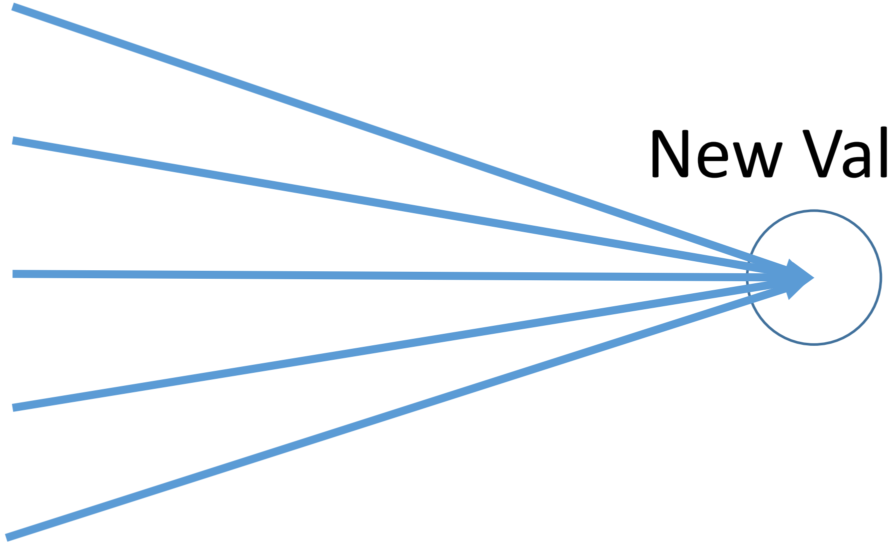
Get value to emerge as quickly as possible



Variation is waste

TOYOTA





Variation is waste

Hansei

Value stream mapping

Andon

A3

Visual management

Jidoka

Genchi genbutsu

Kanban

Ishikawa

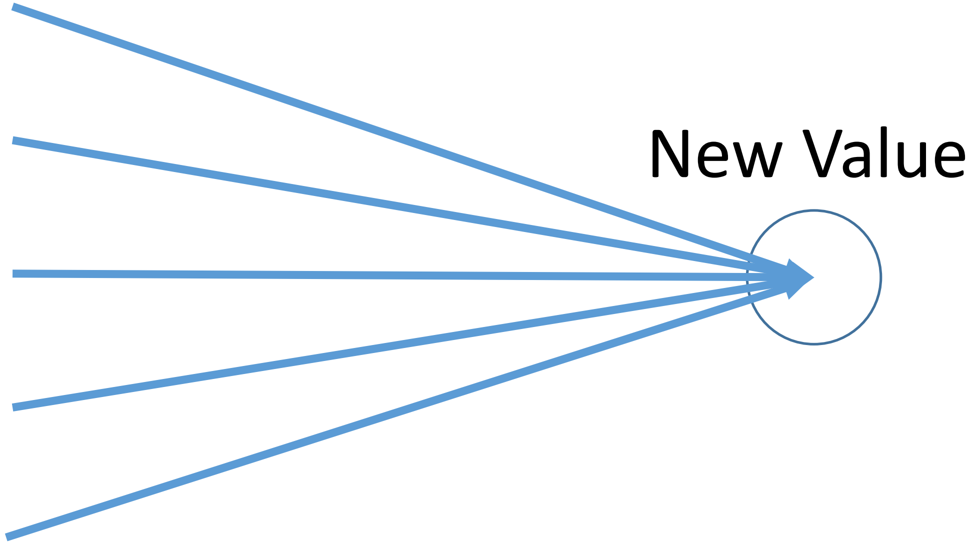
5S

Hoshin Kanri

Yokoten

Kaizen

Poka yoke



Variation is waste *during production*

TOYOTA

Hansei

Value stream mapping

Andon

A3

Visual management

Jidoka

Genchi genbutsu

Kanban

Ishikawa

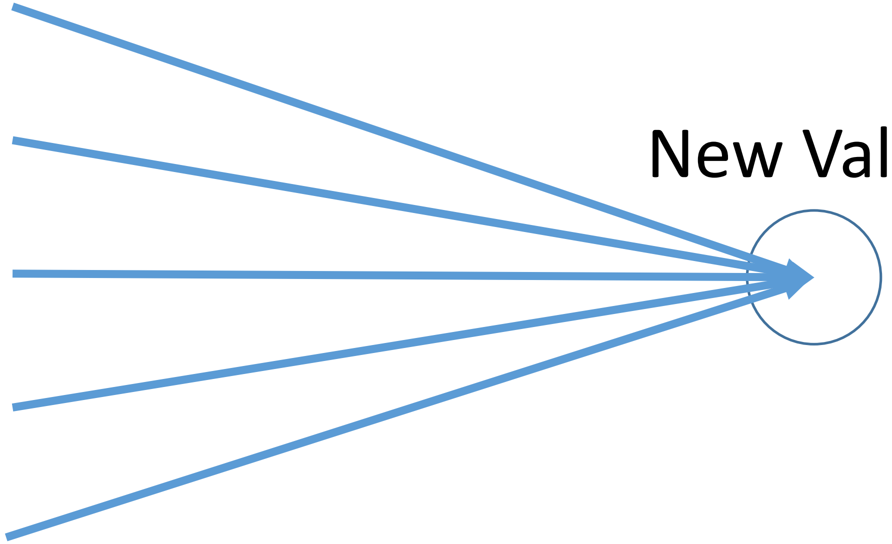
5S

Hoshin Kanri

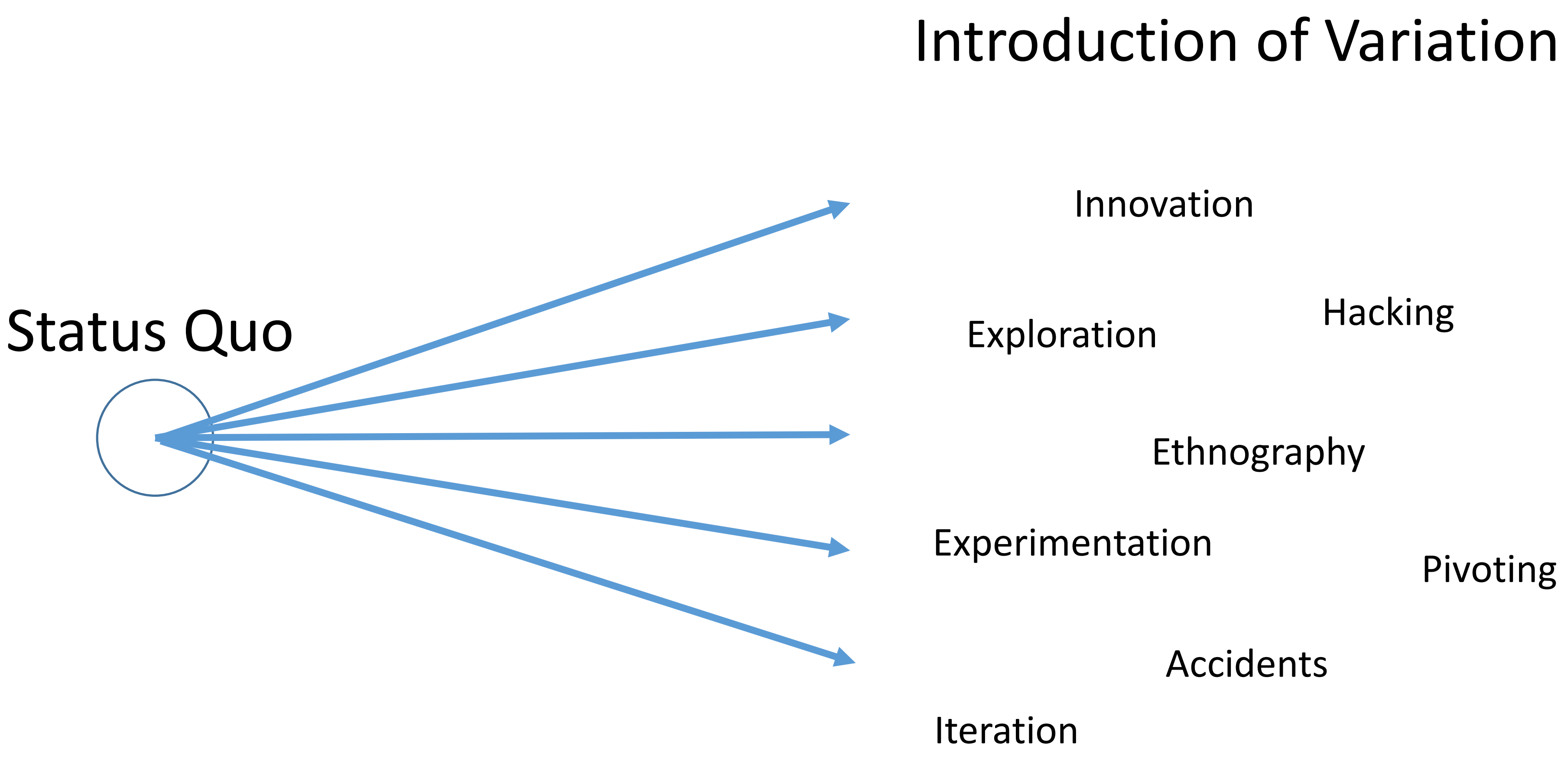
Yokoten

Kaizen

Poka yoke



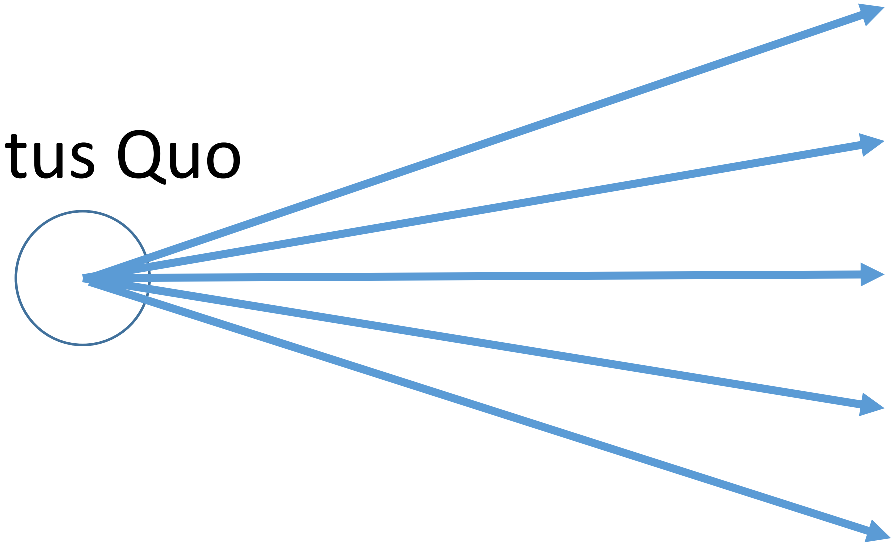
Creation of New Value Requires Introduction of Variation



Successful Creation of New Value Requires *Engineered* Introduction of Variation

Introduction of Variation

Status Quo



Innovation

Design of Experiments

Statistics

Chief Engineer

Hacking

Concept Paper

Exploration

Modeling and Simulation

Ethnography

Lean / Agile

Experimentation

Pivoting

Data Mining

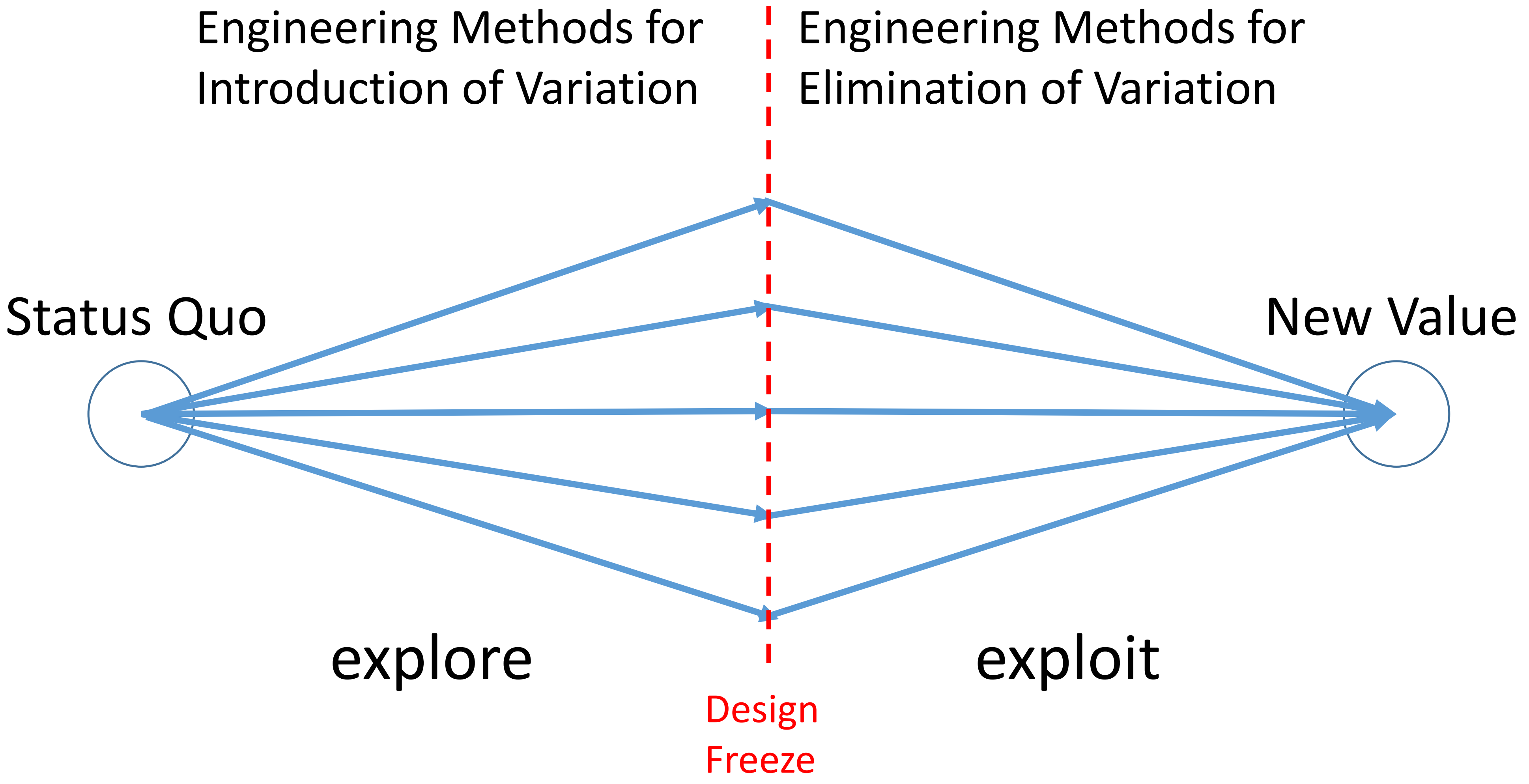
ConOps

Accidents

Iteration

Set-based Concurrent Engineering

The existential question: when to pivot from exploration to exploitation?



We build systems for their emergent properties

Bigfoot System's emergent properties:

- Safety: freedom from accidents (loss)
- Security: making the system impossible for non-designated people to use
- Usability: the ease with which a user can learn / operate the system
- Reliability: freedom from failure
- Supportability: the ease of making changes to the system after deployment

To achieved these properties:

- Model Based Design (MBD)
- Systems Theoretic Process Analysis (STPA)
- Lean / Agile Development
- Modeling and Simulation

Emergent properties will emerge

- You can jump right to an assumed solution and attempt to launch it in the marketplace through repeated surprises and thrashing
- Or you can do the trade studies / concept engineering upfront in a planned, cost-bounded manner

- Either way, you are going to discover the emergent properties / the unknown unknowns

Nonfunctional Requirements of Real-Time Systems

TEREZA G. KIRNER*

Department of Computer Science
Federal University of São Carlos, SP Brazil

ALAN M. DAVIS

El Pomar Chair of Software Engineering
Department of Computer Science
University of Colorado at Colorado Springs

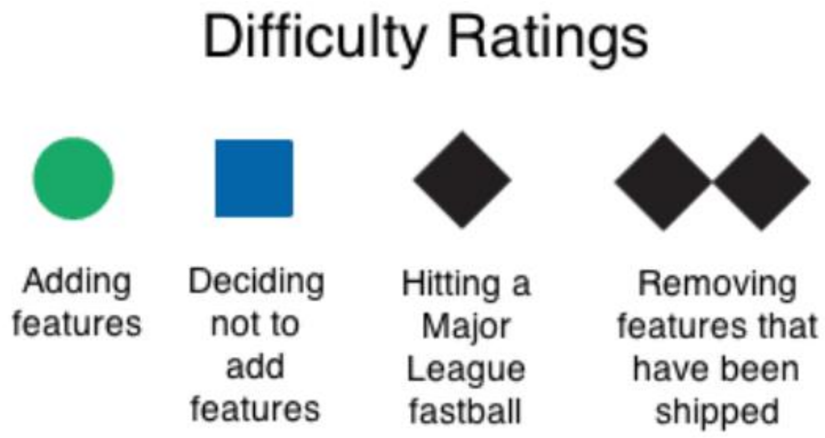
Abstract

A requirements specification typically contains both functional and nonfunctional requirements. Whereas functional requirements address the system's inputs, outputs, and their behavioral interrelationships, nonfunctional requirements define the general qualities of the intended product. The properties of six of the most important nonfunctional requirements for real-time systems are analyzed: timing, reliability, safety, security, usability, and maintainability. For each type of requirement, we define the term, contrast it to other nonfunctional requirements, define how to measure it, define techniques of how to assure its presence, and discuss how to specify the requirement in a requirements specification.

Kirner, Tereza G., and Alan M. Davis. "Requirements specification of real-time systems: temporal parameters and timing-constraints." *Information and Software Technology*38.12 (1996): 735-741.

Complexity is all about variation

- Valuable / Non-valuable
- Antipatterns
- Tight coupling, low cohesion
- Technical debt
- Domain complexity / accidental complexity
- Slows things down, makes them more expensive



Non-value-added variation; avoiding over-serving

"If you're not the simplest solution, you're the target of one"

Development cost

Development time

Marketing effort

Training costs

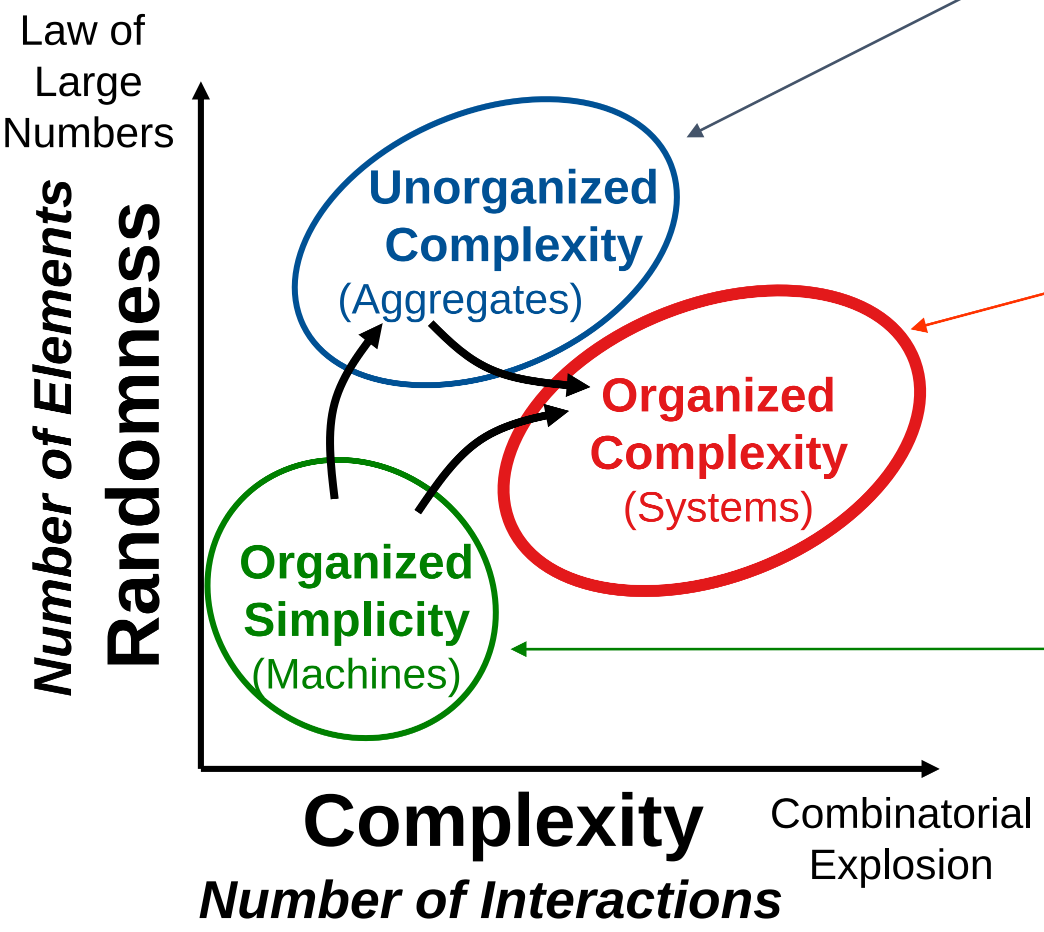
Support costs

Dependability (safety, reliability, usability)

Regulatory speed

Competitive position

Machines, Aggregates, Systems



Unorganized Complexity (Aggregates)

- Chemistry
- Law of large numbers
- Black box
- Sufficiently random
- Lack underlying structure therefor reductionism ineffective
- "Design by Statistics"

Organized Complexity (Systems)

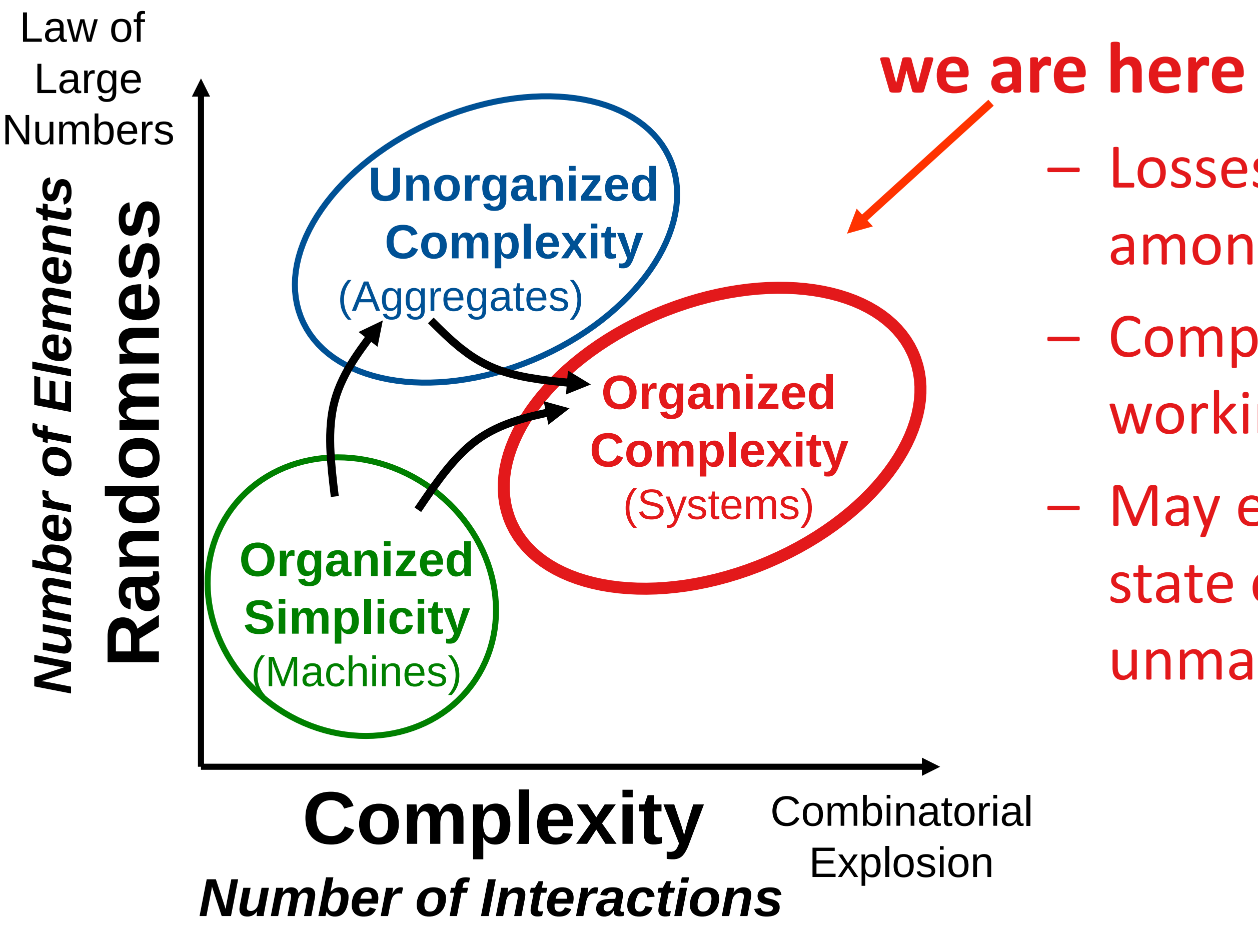
- Neither chemistry nor physics
- Grey box
- Law of medium numbers
- Human behavior
- Software behavior
- Too complex for analysis while being too organized for statistics

Organized Simplicity (Machines)

- Simple enough to be analyzed (chopped into small pieces)
- Physics
- Law of small numbers
- White box
- Not random
- Well described by equations
- Limited interactions
- "Design by Detail"

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18.

Machines, Aggregates, Systems

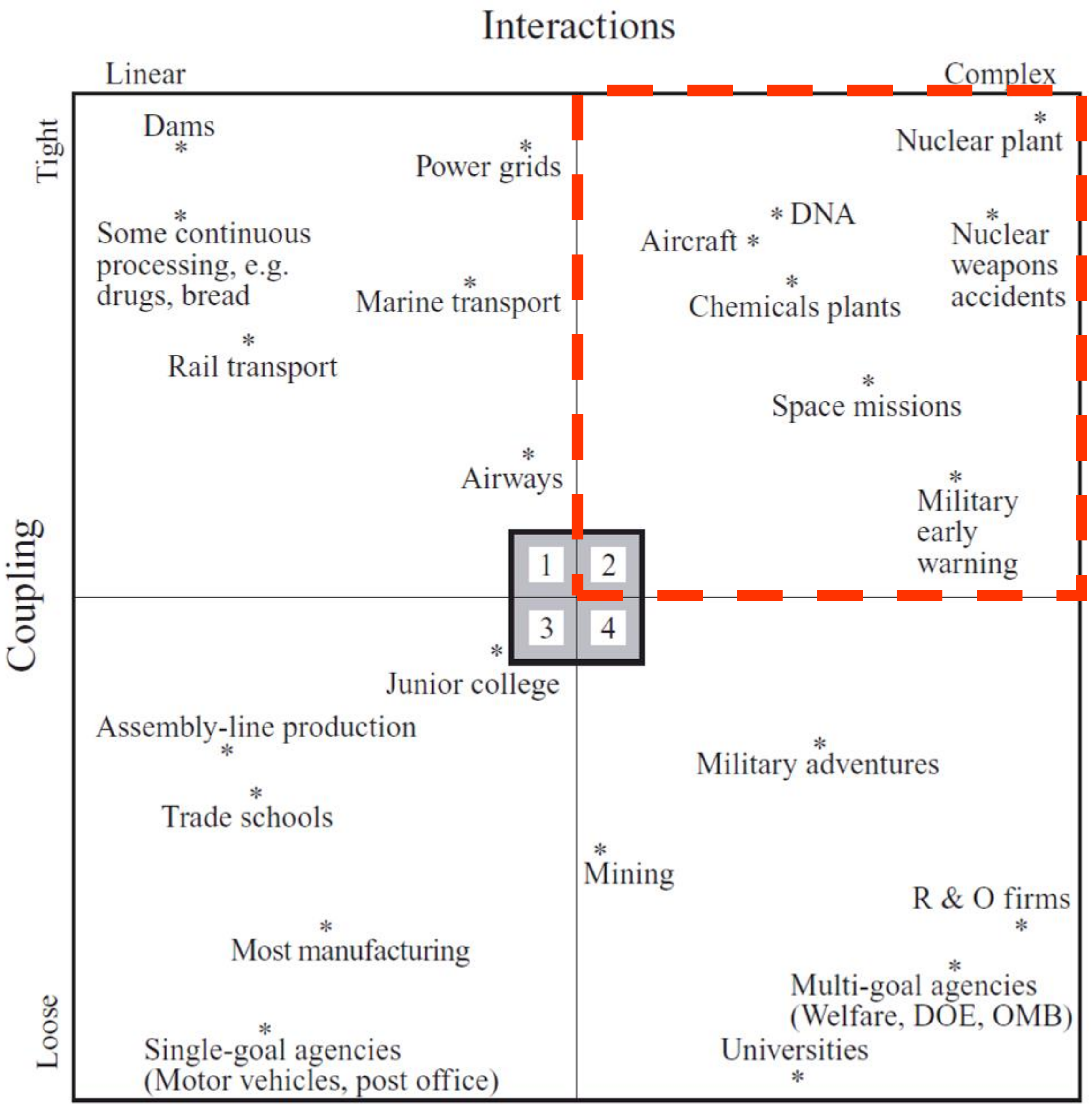


- Losses due to interactions amongst components
- Components are often working fine / reliable
- May evolve to an unsafe state over time, due to unmanaged change

From: G.M. Weinberg, An Introduction to General Systems Thinking, John Wiley & Sons, New York, 1975, p 18.

Hazards + Humans + Software + Feedback =

Be Careful!



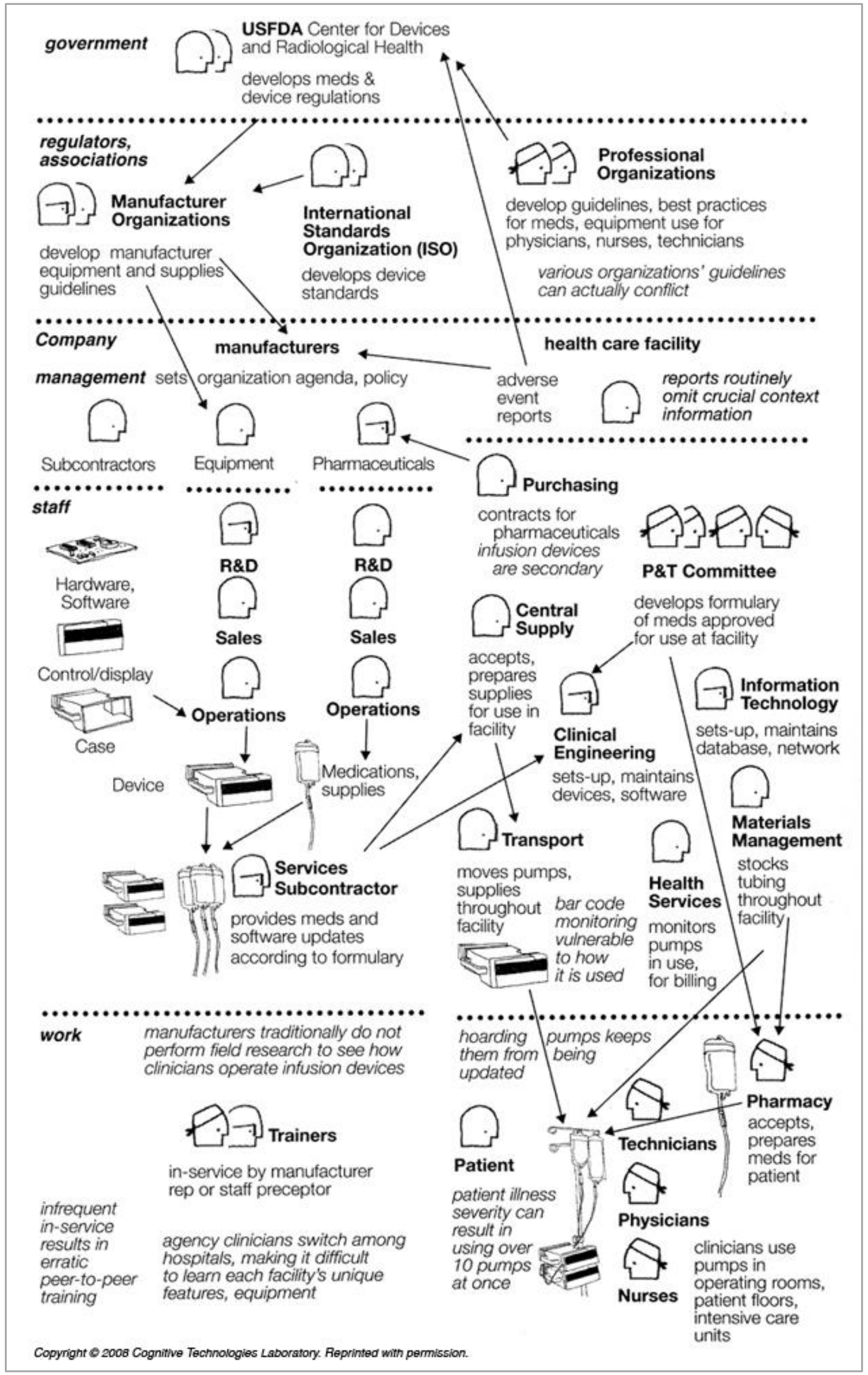
Charles Perrow, "Normal Accidents: Living with High-Risk Technologies" (1984)


CURLIN MEDICAL
4000 CMS™
ON OFF
RUN
STANDBY
ALARM
HELP
OPTIONS
RUN
PAUSE
NO
CHANGE
YES
ENTER
1
2
3
4
5
6
7
8
9
0
SILENCE
PRIME
BOLUS

An infusion pump is a system

"An infusion "device," the most widely used information technology (IT) in health care, is actually an interdependent network of relationships. It's a socio-technical system that spans all who develop, supply, and use the result, from the level of the care provider or manufacturer organization, to associations and regulators, to government. This requires a different approach to safety: at the systems, not the device, level."

– Christopher Nemeth



Sources:

- Nemeth C, "The Safety of Medical Devices Perspective", http://www.webmm.ahrq.gov/perspective.aspx?perspectiveId=104
- Nemeth C, Cook R. The infusion device as a source of resilience. In Nemeth C, Hollnagel E, Dekker F, Dekker S, eds. Resilience Engineering Perspectives, 2. Farnham, UK: Ashgate Publishing; 2009. ISBN: 9780754675204. Preparation and Restoration; vol 2.

Complexity is the enemy

1. It appears that the outcome of current system engineering practice is complexity - especially development of large-scale systems
2. Interactive complexity: Property of interactiveness between parts of the system (planned or unplanned interactions)
3. Tightly coupled systems have more time-dependent processes: What happens in one part directly affects what happens in the other
4. If the systems being developed are complexly interactive and tightly coupled, by nature they are risky and prone to failure (Charles Perrow, System Accident Theory)
5. "The main problem is complexity itself"
6. This creates space for effective project management practices facilitated by knowledge management mechanisms & technologies
7. Increased project complexity implies that no one individual or team can at a given time comprehend the entire system that is being developed

Source: Role of knowledge management in project management of complex systems organizations, NASA JSC Conference, Arvind Gudi, March 2-3, 2006

"The future is already here, it just hasn't been evenly distributed yet"
– William Gibson

1. Don't Be Intimidated By New Industries
2. Mysteries and Puzzles
3. Connect, Connect, Connect
4. Keep You Feet On The Ground And Your Head In The Clouds
5. Read, Read, Read
6. Questions And Answers
7. Lifelong Learning
8. Quiet
9. Laws
10. Don't Spend Time On The Summits

Thank you

Notes

- Best way to contact me: Ldesborough@bigfootbiomedical.com
- More about designing safe cyberphysical systems
  - https://aamiblog.org/2013/07/30/lane-desborough-the-value-of-simplicity-in-a-complex-world/
  - http://psas.scripts.mit.edu/home/get_pdf.php?name=2-1-Desborough-Using-STPA-in-the-Development-of-an-Artificial-Pancreas.pdf
- More about Bigfoot:
  - https://www.mathworks.com/videos/developing-an-artificial-pancreas-using-model-based-design-1481554386617.html slides and video
  - https://www.bigfootbiomedical.com/vision/
  - https://www.bigfootbiomedical.com/podcasts/
  - https://www.bigfootbiomedical.com/news/

Ancestor Effect*

“Much like biological genealogy, academic 'ancestors' pass on certain traits and attitudes to their offspring. By tracing our pasts, we may understand our present a bit more thoroughly”

- Charles Danforth

*Fischer, Peter, Anne Sauer, Claudia Vogrincic, and Silke Weisweiler. "The ancestor effect: Thinking about our genetic origin enhances intellectual performance." *European Journal of Social Psychology* 41, no. 1 (2011): 11-16.

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

George Box

McMaster University

John MacGregor

Queen's University

Thomas Harris

Kim McAuley

me

Jim McLellan

Zahra Eghtesadi

References

- The Systems Bible - Gall
- Engineering a Safer World - Leveson
- Product Development Flow – Reinertsen
- Our Robots, Ourselves - Mindell
- A list of my books (200+), rated: https://www.goodreads.com/review/list/1114014

A model is not reality. - Rechtin's heuristics for system architecting

Complex systems exhibit unexpected behavior. - The Systems Bible

Every once in a while you have to go back and see what the real world is telling you. [Harry Hillaker, 1993] - Rechtin's heuristics for system architecting

Overengineering: Spending resources making a project more robust and complex than is needed

Just because it worked in the past there’s no guarantee that it will work now or in the future. (Kenneth L. Cureton, 1991) - Rechtin's heuristics for system architecting

Reality is more complex than it seems. - The Systems Bible

The Kantian Hypothesis (Know-Nothing Theorem): Large complex systems are beyond human capacity to evaluate. - The Systems Bible

Magic numbers: Including unexplained numbers in algorithms

Choose the elements so that they are as independent as possible; that is, elements with low external complexity (low coupling) and high internal complexity (high cohesion). - Rechtin's heuristics for system architecting

Don’t assume that the original statement of the problem is necessarily the best, or even the right, one.   - Rechtin's heuristics for system architecting

New systems mean new problems. - The Systems Bible

In order to understand anything, you must not try to understand everything. (Aristotle, 4th cent. B.C.)   - Rechtin's heuristics for system architecting

Errors are most frequent during the requirements and design activities and are the more expensive the later they are removed. - Boehm' Law

Plan to scrap the first system: You will anyway. - The Systems Bible

If you can’t explain it in five minutes, either you don’t understand it or it doesn’t work. (Darcy McGinn, 1992 from David Jones) - Rechtin's heuristics for system architecting

Individual developer performance varies considerably. - Sackman' Law

The Fundamental Theorem: New systems generate new problems.
- The Systems Bible

The total behavior of large systems cannot be predicted. - The Systems Bible

Premature optimization: Coding early-on for perceived efficiency, sacrificing good design, maintainability, and sometimes even real-world efficiency

Simplify, combine, and eliminate. (Suzaki, 1987) - Rechtin's heuristics for system architecting

Big ball of mud: A system with no recognizable structure

Kaplan's Law of the Instrument - Give a small boy a hammer and he will find that everything he encounters needs pounding.

“A complex system that works is invariably found to have evolved from a simple system that works”
– John Gaule

Everything is a system. - The Systems Bible

A complex system designed from scratch never works and cannot be patched up to make it work. You have to start over, beginning with a working simple system. - The Systems Bible

"The future is already here. It just hasn't been evenly distributed yet" - William Gibson

A structure is stable if cohesion is strong and coupling low. - Constantine' Law

The first line of defense against complexity is simplicity of design.
- Rechtin's heuristics for system architecting

A system is no better than its sensory organs. - The Systems Bible

Unbounded limits on element behavior may be a trap in unexpected scenarios. [Bernard Kuchta, 1989] - Rechtin's heuristics for system architecting

Build reality checks into model-driven development. [Larry Dumas, 1989] - Rechtin's heuristics for system architecting

Simplify. Simplify. Simplify. - Rechtin's heuristics for system architecting

High quality, reliable systems are produced by high quality architecting, engineering, design, and manufacture, not by inspection, test, and rework. - Rechtin's heuristics for system architecting

An evolving system increases its complexity, unless work is done to reduce it. - Lehman' Law

If things are acting very strangely, consider that you may be in a feedback situation. - The Systems Bible

Complicated systems produce complicated responses to problems. - The Systems Bible

Relationships among the elements are what give systems their added value. - Rechtin's heuristics for system architecting

"All other things being equal, the simplest solution is the best." - Occam's razor

If the politics don’t fly, the hardware never will. (Brenda Forman, 1990)   - Rechtin's heuristics for system architecting

Technical problems become political problems.   - Rechtin's heuristics for system architecting

If you can’t analyze it, don’t build it.   - Rechtin's heuristics for system architecting

Stockdale Paradox: "You must never confuse faith that you will prevail in the end – which you can never afford to lose – with the discipline to confront the most brutal facts of your current reality, whatever they might be."

In introducing technological and social change, how you do it is often more important than what you do. - Rechtin's heuristics for system architecting

Lava flow: Retaining undesirable (redundant or low-quality) code because removing it is too expensive or has unpredictable consequences[5][6]

“Simplicity is an acquired taste. Mankind, left free, instinctively complicates life.” - Katherine F. Gerould

Hierarchical structures reduce complexity. - Simon' Law

Connect-the-Dots Principle: There must be a traceable connection from business strategy to each enterprise architecture decision. - Dana Bredemeyer

Accidental complexity:
Introducing unnecessary
complexity into a solution

The value of models depends on the view taken, but none is best for all purposes. - Davis' Law

Without data, discussions produce more heat than light - Edwards Deming

Performance, cost, and schedule cannot be specified independently. At least one of the three must depend on the others.
- Rechtin's heuristics for system architecting

A combination of different V&V methods outperforms any single method alone. - Hetzel–Myers' Law

Minimalist Architecture Principle: Make only those decisions that have to be made at this level of scope to achieve the business strategy and meet the architecture objectives and vision.
- Dana Bredemeyer

Decisions With Teeth Principle: Only include decisions in your Enterprise Architecture that you, and the governance organization, are willing and able to enforce. - Dana Bredemeyer

In architecting a new [software] program all the serious mistakes are made in the first day. [Spinrad, 1988]   - Rechtin's heuristics for system architecting

Development effort is a (non-linear) function of product size. - Boehm' Law

“Simplicity is the ultimate sophistication” - Leonardo da Vinci

Choose a configuration with minimal communications between the subsystems. (computer networks) - Rechtin's heuristics for system architecting

"Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius -- and a lot of courage -- to move in the opposite direction."

- Albert Einstein

Sinclair’s Law - If a man's paycheck depends on his not understanding something, you can rely upon his not understanding it

Requirement deficiencies are the prime source of project failures. - Glass' Law

“If you don't have time to do it right, when will you have time to do it over?” – John Wooden