



Aalto University

Lecture 4: Errors and Complexity

ELEC-D7010 Engineering for Humans

April 29, 2021

Antti Oulasvirta

Aalto University

10 Apr 2019 | 10:49 am

How the Boeing 737 Max Disaster Looks to a Software Developer

Design shortcuts meant to make a new plane seem like an old, familiar one are to blame

By **Gregory Travis**

The views expressed here are solely those of the author and do not represent positions of IEEE Spectrum or the IEEE.

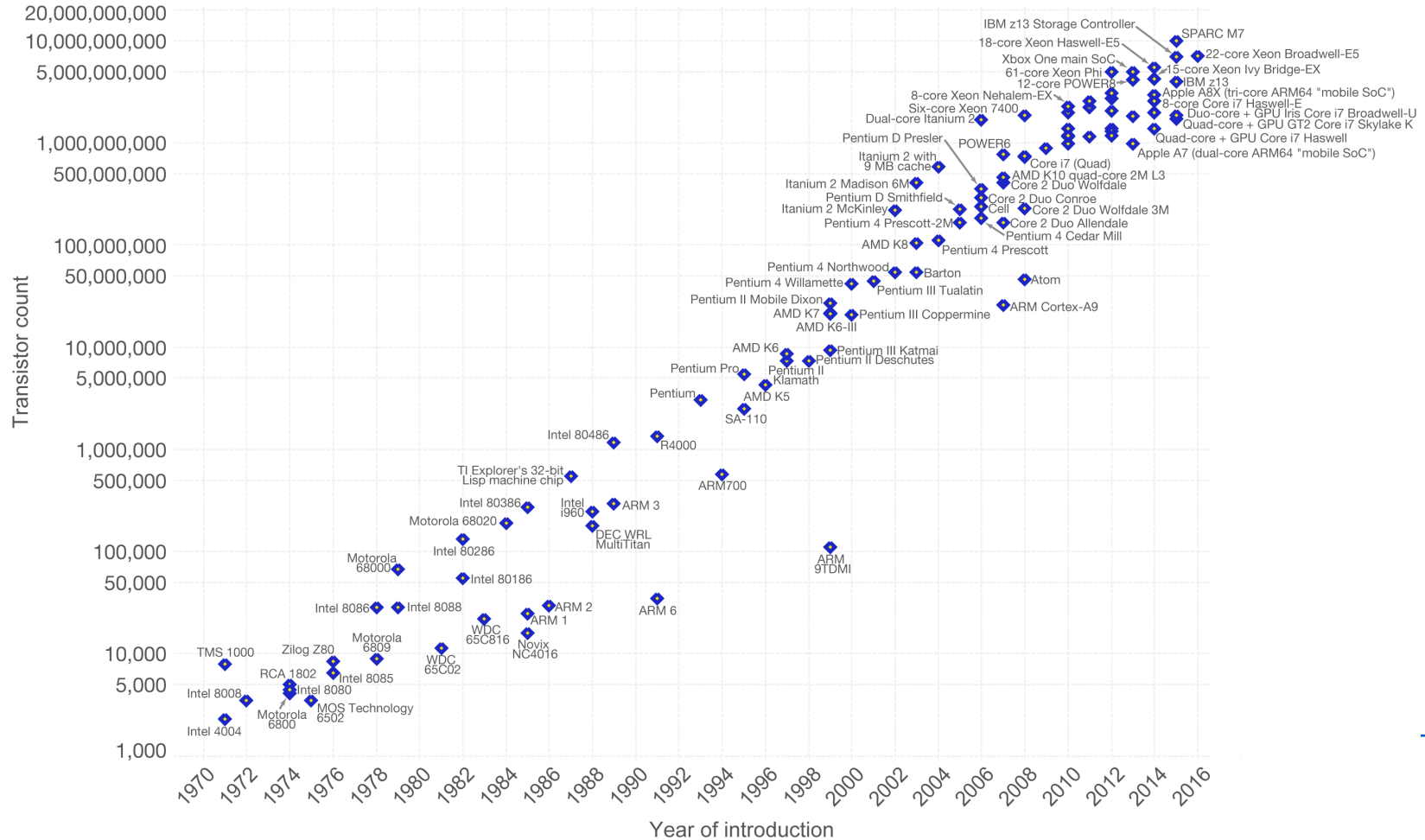


Photo: Jemal Countess/Getty Images

This is part of the wreckage of Ethiopian Airlines Flight ET302, a Boeing 737 Max airliner that crashed on 11 March in Bishoftu, Ethiopia, killing all 157 passengers and crew.

Moore's Law – The number of transistors on integrated circuit chips (1971-2016)

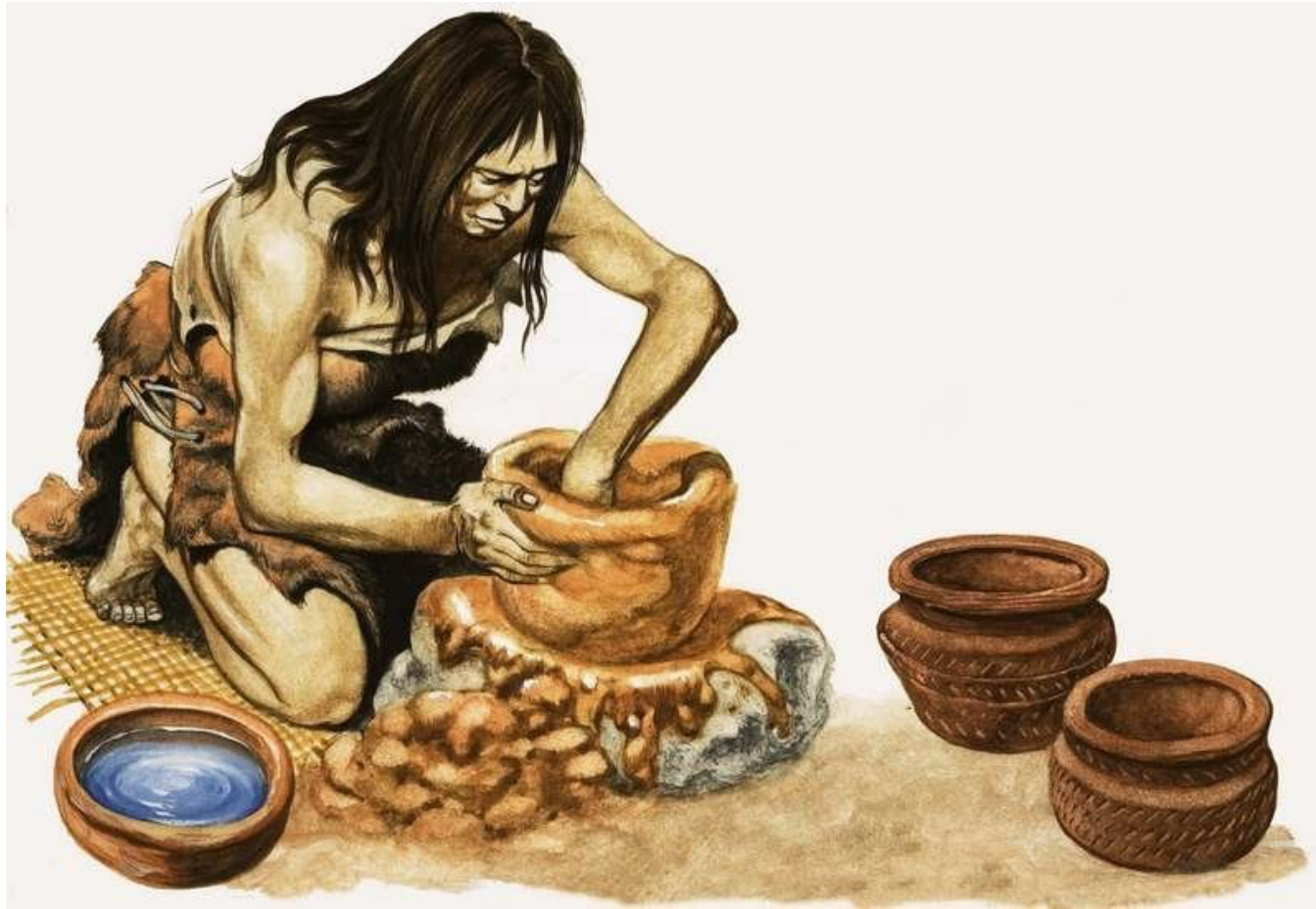
Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are strongly linked to Moore's law.



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)

The data visualization is available at [OurWorldinData.org](https://ourworldindata.org). There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.



Topics today



- 1. Implications of Complexity**
- 2. Human Error**
- 3. Task Analysis**

Learning objectives today

1. Complex systems and failures

What makes systems fail

Typical causes and consequences of failure

2. Causes of human error

Overview: Theories of human error in complex system use

Rasmussen's SRK

Skills, Rules, Knowledge

3. Task analysis

Decomposition of complex activities into simple constituents

Hierarchical Task Analysis

Assignment 4: Preview

A4-1: Task analysis [5p, recommended]

A4-2: Root cause analysis of an accident [5p, optional]



Aalto University

1. Complexity and System Reliability

In this section

Complex systems in general

What makes them brittle: Human factors

Understanding failure



Aalto University

Complex systems



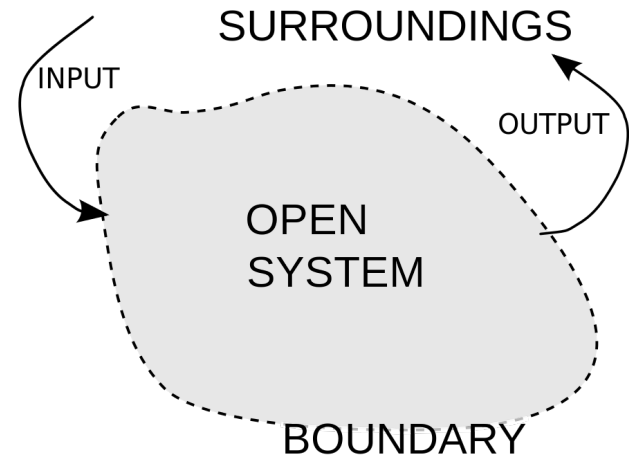
Q: Name a very complex system

Q: Name a very complex system that does NOT involve a human operator/user

Q: What is a complex system?

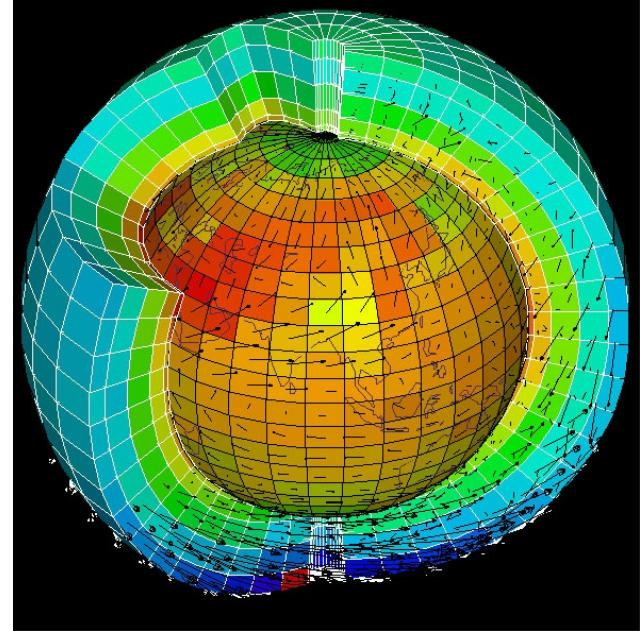
What is a system?

- **A system is a set of elements and their interactions that form a whole**
- **It is defined by means of a boundary which determines entities that are not part of the system**
- **A system can exhibit system-level behaviors that do not reduce to its elements**



Complex system

- **A complex system is a system composed of many components which interact with each other.**
- **Intrinsically hard to model due to large number of inter-dependencies.**
- **Complex systems have emergent properties, such as nonlinearity, spontaneous order, adaptation, feedback loops, stability, ...**



Example: A climate model



Q: What is a *system* here?

Control room of the Lausward Power Plant

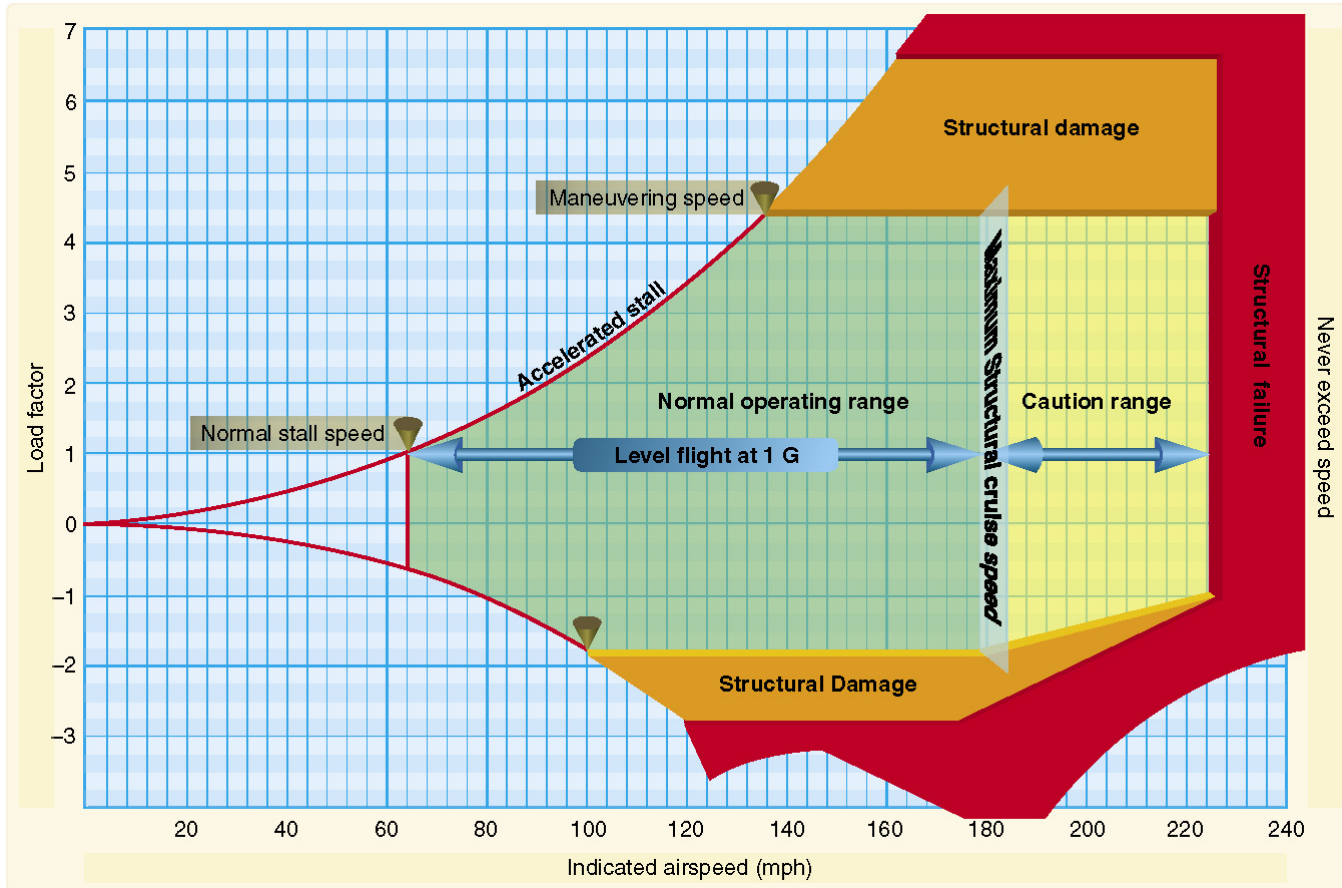




Aalto University

Humans and complex systems

Complex systems have multi-dimensional operating envelopes

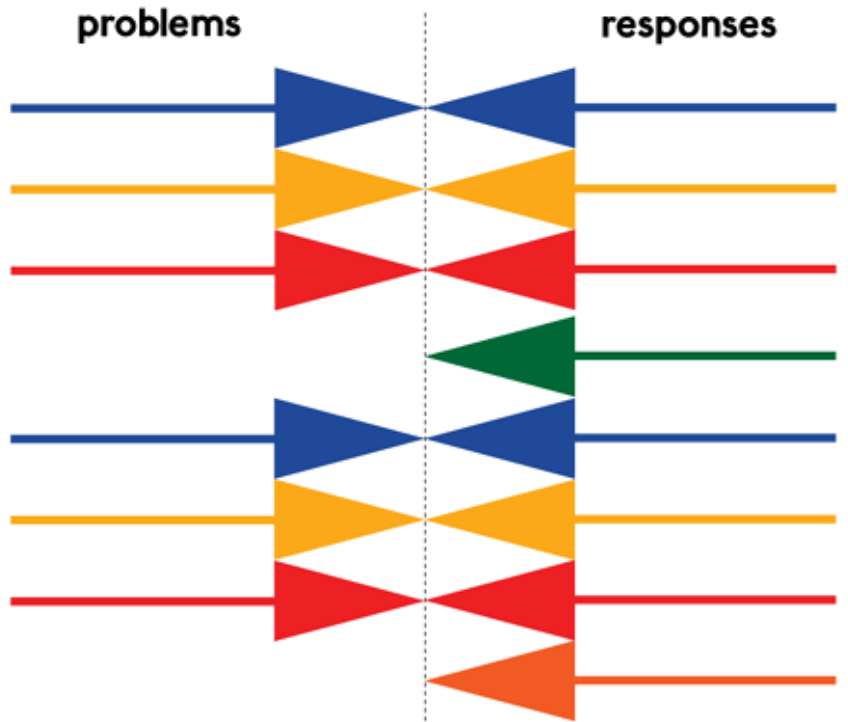


To control complex behavior, a matching level of complexity in the controller is needed

Example: Thermostat



Law of Requisite Variety



requisite variety: (at least) the right variety in responses to deal with variety of the problems

A successful control system (e.g., user) must be capable of entering at least as many states as the system being controlled: “only variety can force down variety” (W. Ross Ashby 1956).

Roger Conant: “Every good regulator of a system must be a model of that system”

Law of Requisite Variety in practice



To set a desirable level of temperature, the user needs to predict how “Set temperature”, “Fan”, and “System” affect the experienced temperature together with the room climate



Why do people fail to match requisite variety?

Lack of skill

Lack of knowledge

Lack of awareness

Poor judgment

Unsafe acts, errors, mistake

Overreliance on automation

Automation surprises

....



Aalto University

Understanding failure

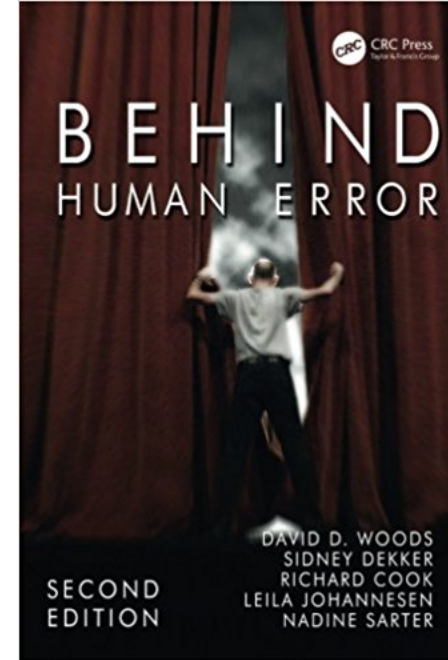
**Good to
Know**

Richard I. Cook

How Complex Systems Fail (2002)

The Complexity of Human Error (1994)

Behind Human Error (2010)



1. Complex systems are intrinsically risky

The presence of risk drives the creation of defenses against it.
Think: Healthcare, power plants, banking, aeroplanes, ...



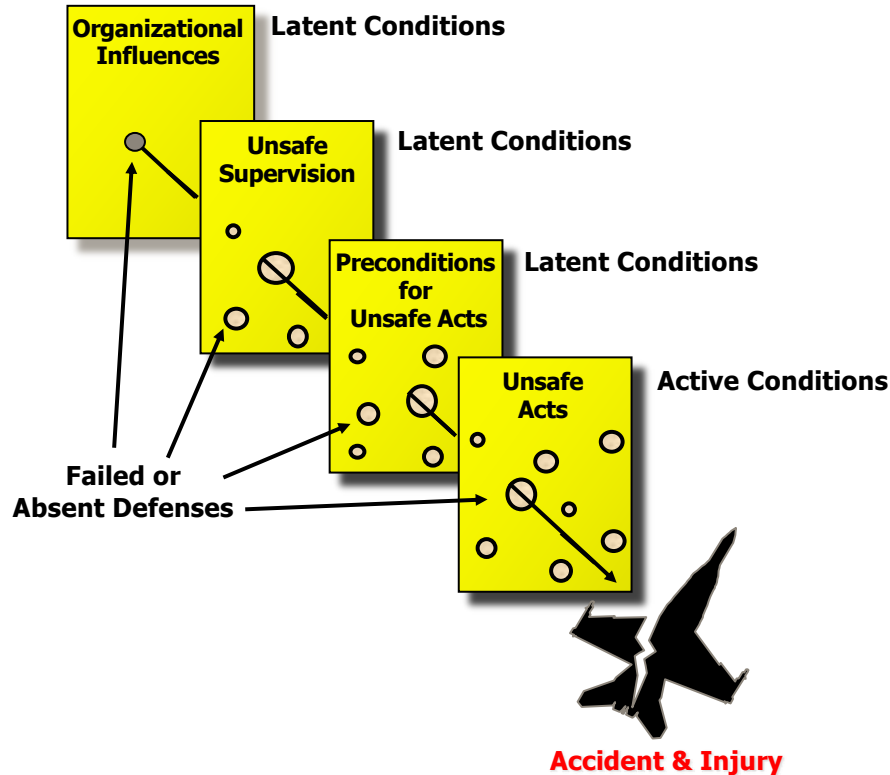
2. Successful systems have *multiple* defenses against failure

Technical (testing, backup systems), human factors (UI design, training), and legal defenses



3. Catastrophes involve multiple failures

There are more failure opportunities than actual failures



“The Swiss cheese model”

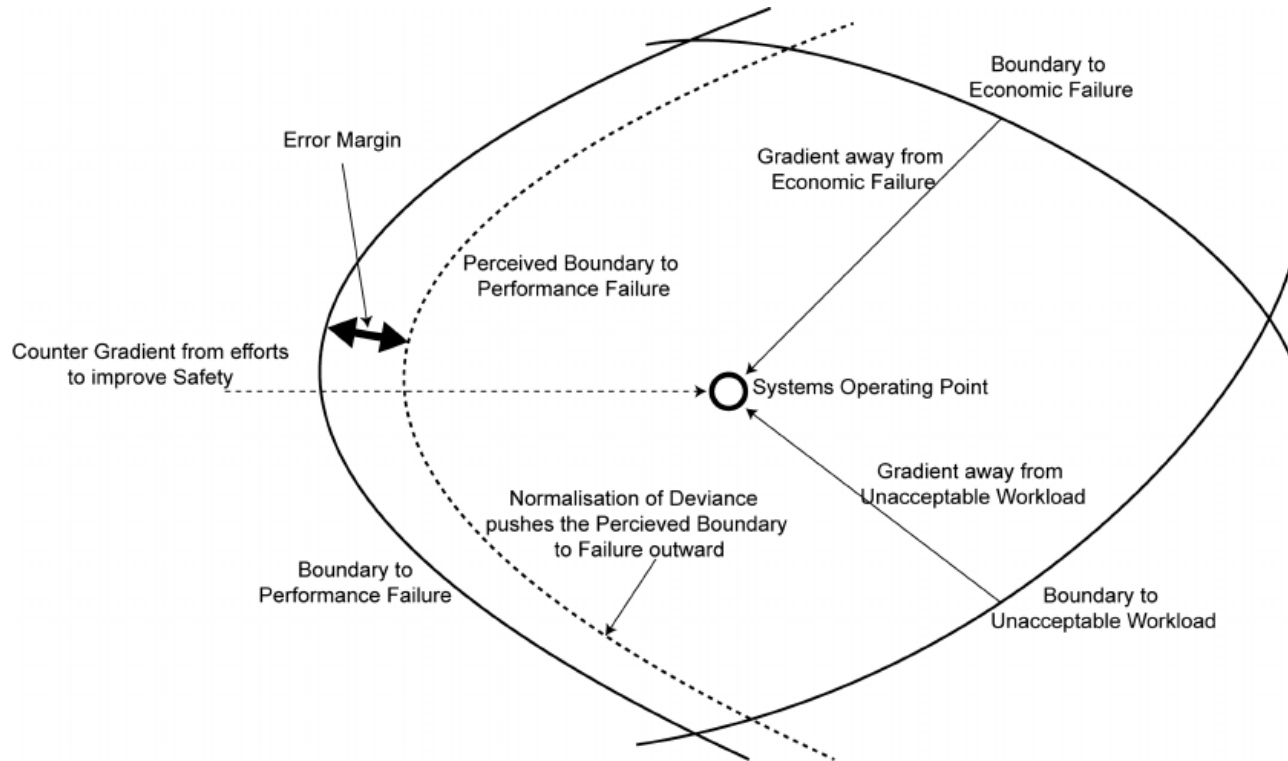
4. Complex systems always involve multiple latent potentials for failure

All failures impossible to remove. The failures change constantly due to technology, human practices, and R&D



5. Complex systems often operate close to failure point

Complex systems are often run as broken systems, which is possible due to multiple redundancies.



6. Post-accident attribution to a “root cause” is challenging / misleading

Isolated causes for accidents are often politically motivated attempts at “blaming”



7. Hindsight biases post-accident assessment

Knowledge of the outcome makes it seem that events leading to the outcome should have appeared more salient to practitioners at the time than was actually the case.



8. Human operators both produce and defend against failures

An outsider may misapprehend the operator's constant, simultaneous engagement with both roles.



9. All practitioner actions are gambles

Practitioner actions take place in the face of uncertain outcomes. The degree of uncertainty may change.



10. Humans are the most adaptable element of complex systems

These adaptations include:

- (1) Restructuring the system in order to reduce exposure of vulnerable parts to failure.**
- (2) Concentrating critical resources in areas of expected high demand.**
- (3) Providing pathways for retreat or recovery from expected and unexpected faults.**
- (4) Establishing means for early detection of changed system performance in order to allow graceful cutbacks in production or other means of increasing resiliency.**

11. Change introduces new forms of failure



When new technologies are used to eliminate well understood system failures or to gain high precision performance they often introduce new pathways to large scale, catastrophic failures.

12. “Safety” is characteristic of joint human-system performance



Safety is an emergent property of systems; it does not reside in a person, device or department of an organization or system

13. Failure-free operations require experience with failure



More robust system performance arises in systems where operators discern the “edge of the envelope”. This is where system performance begins to deteriorate, becomes difficult to predict, or cannot be readily recovered.

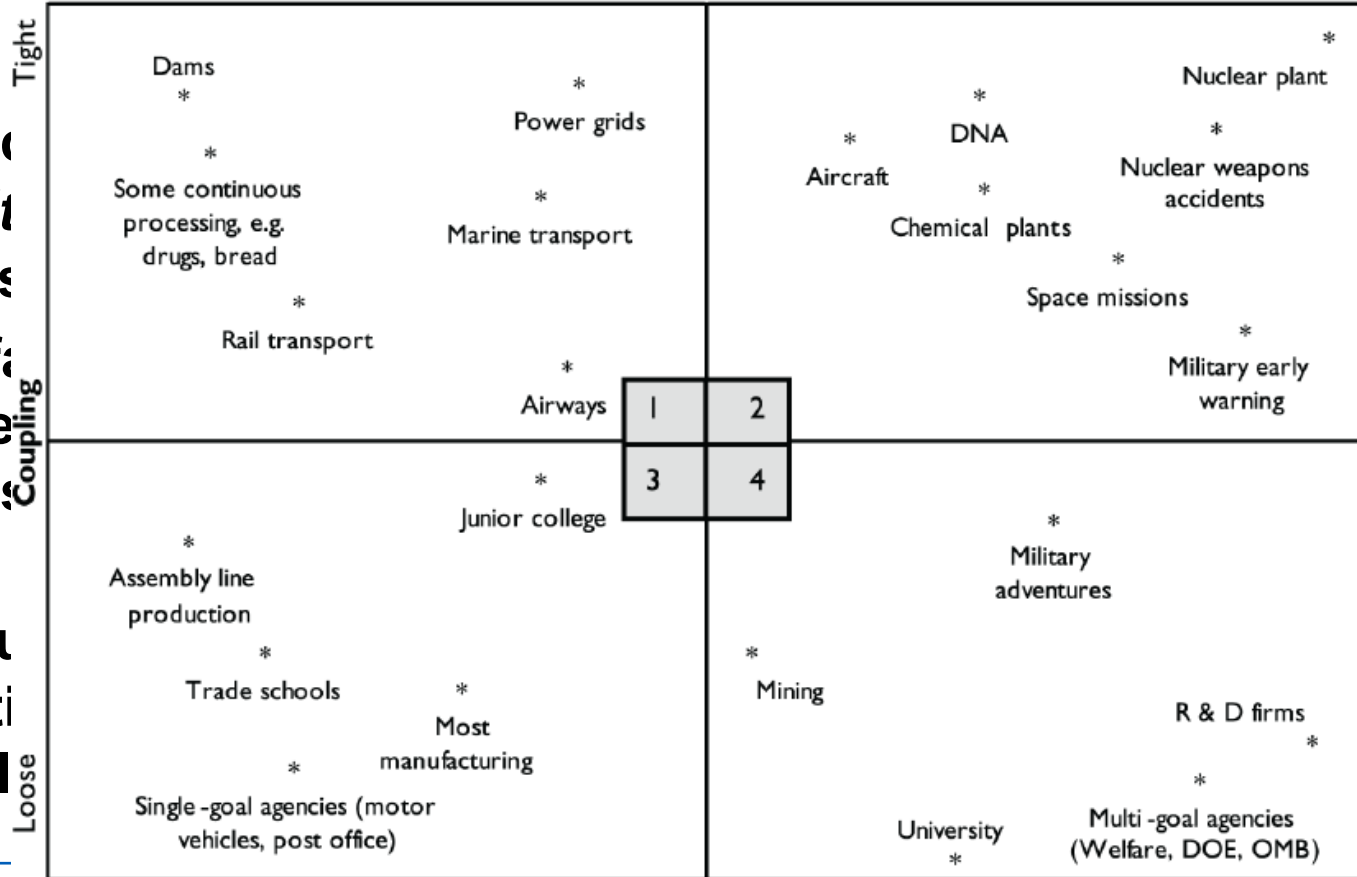
“Normal accidents”

Linear

Interactions

Complex

System are
and inevitable
 complex systems
 Multiple factors
 each other
 occur, design
 them.
 Many failures
 organizational
 very small





Aalto University

Risk and accident analysis methods

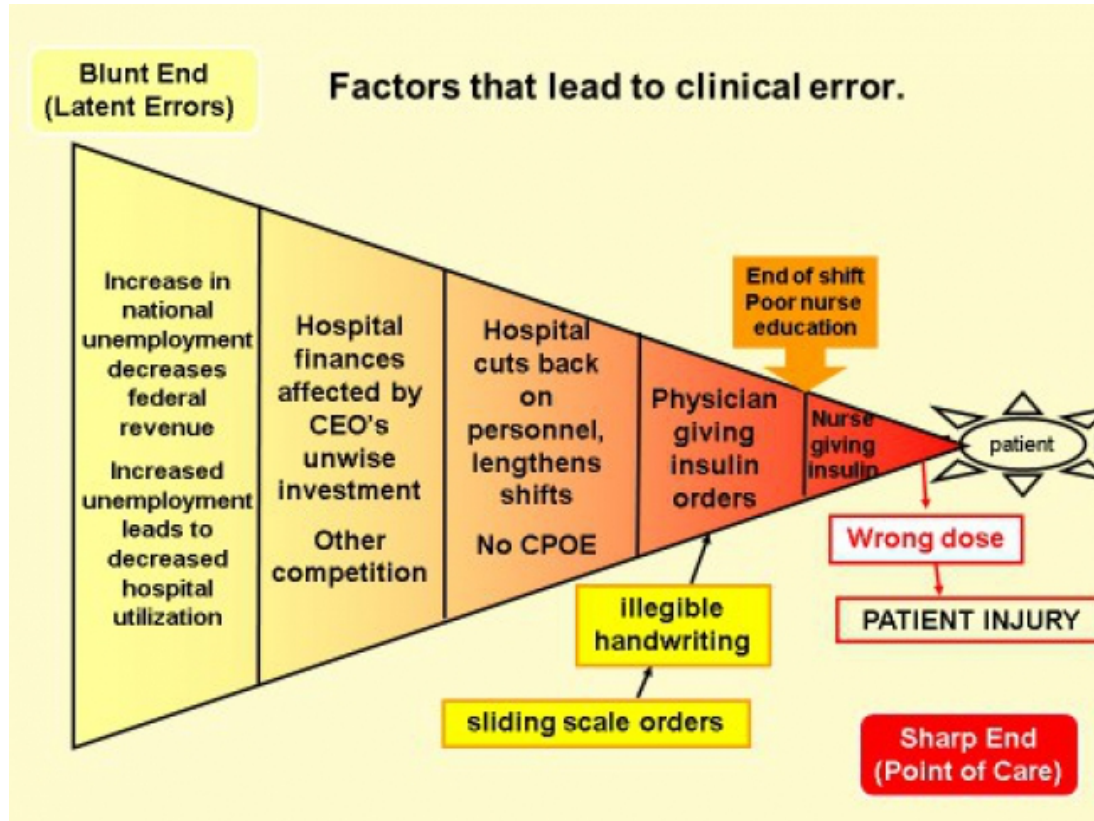
Risk vs. accident analysis

Pre vs. post risk analysis

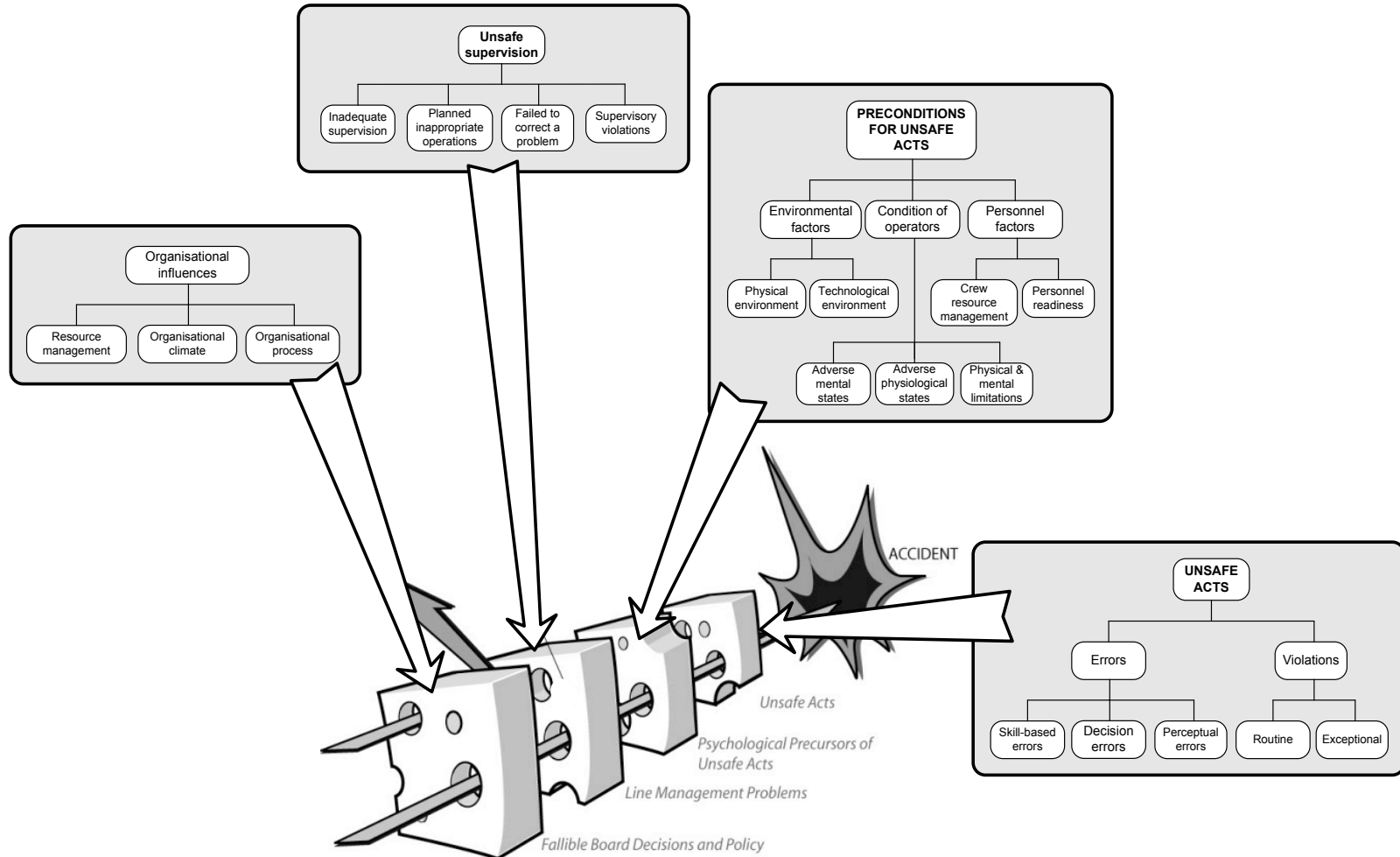


Sharp end vs. blunt end

Visible errors only part of the causal chain. The goal of analysis is to identify the LATENT factors

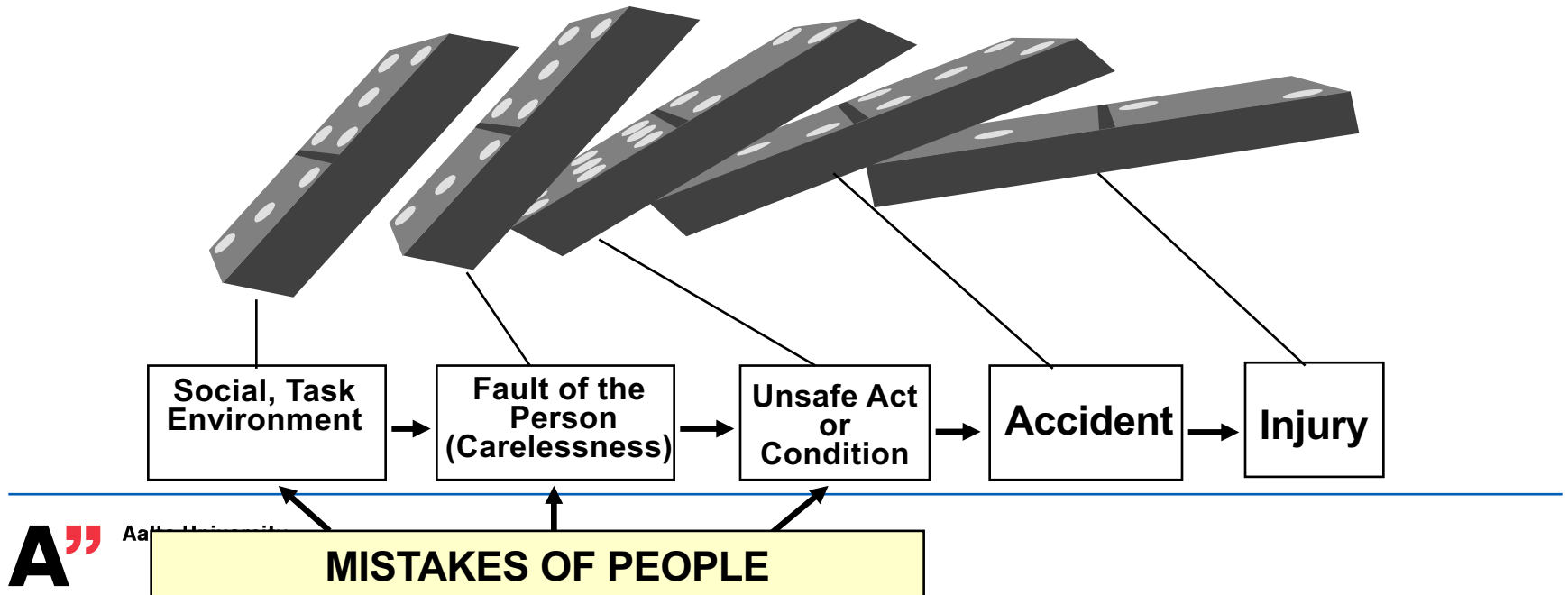


“The Swiss Cheese model”

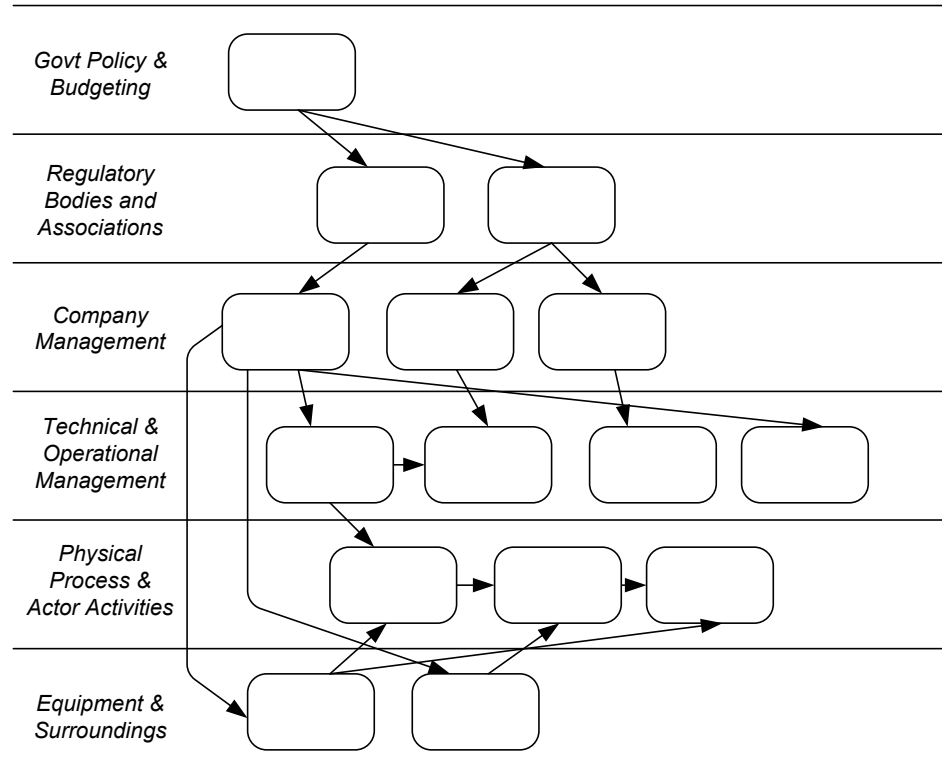
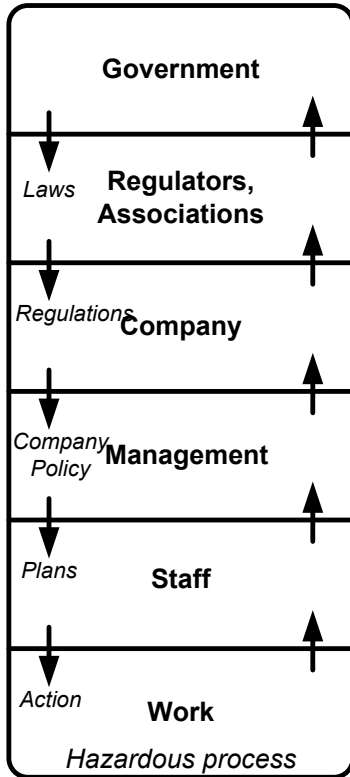



Domino theory

1932 First Scientific Approach to
Accident/Prevention - H.W. Heinrich
“Industrial Accident Prevention”



Accimap method for risk management and accident analysis (Rasmussen)



 = Failures, decision, actions etc

Root Cause Analysis (RCA)

A tool in the systems approach to prevention, not punishment, of adverse events

A tool in the effort to build a “culture of safety”

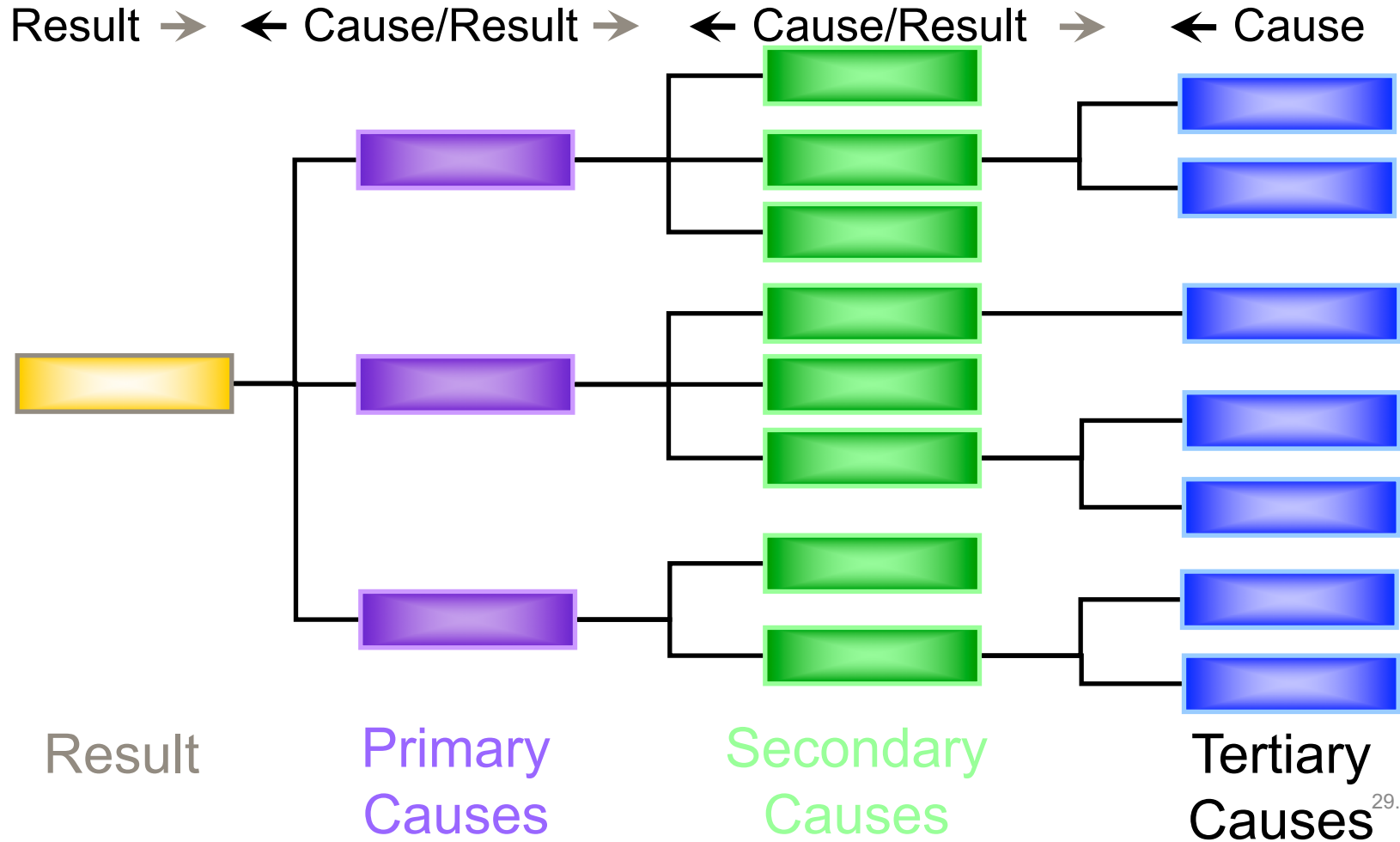
A process for identifying basic or contributing causes

A process for identifying what can be done to prevent recurrence

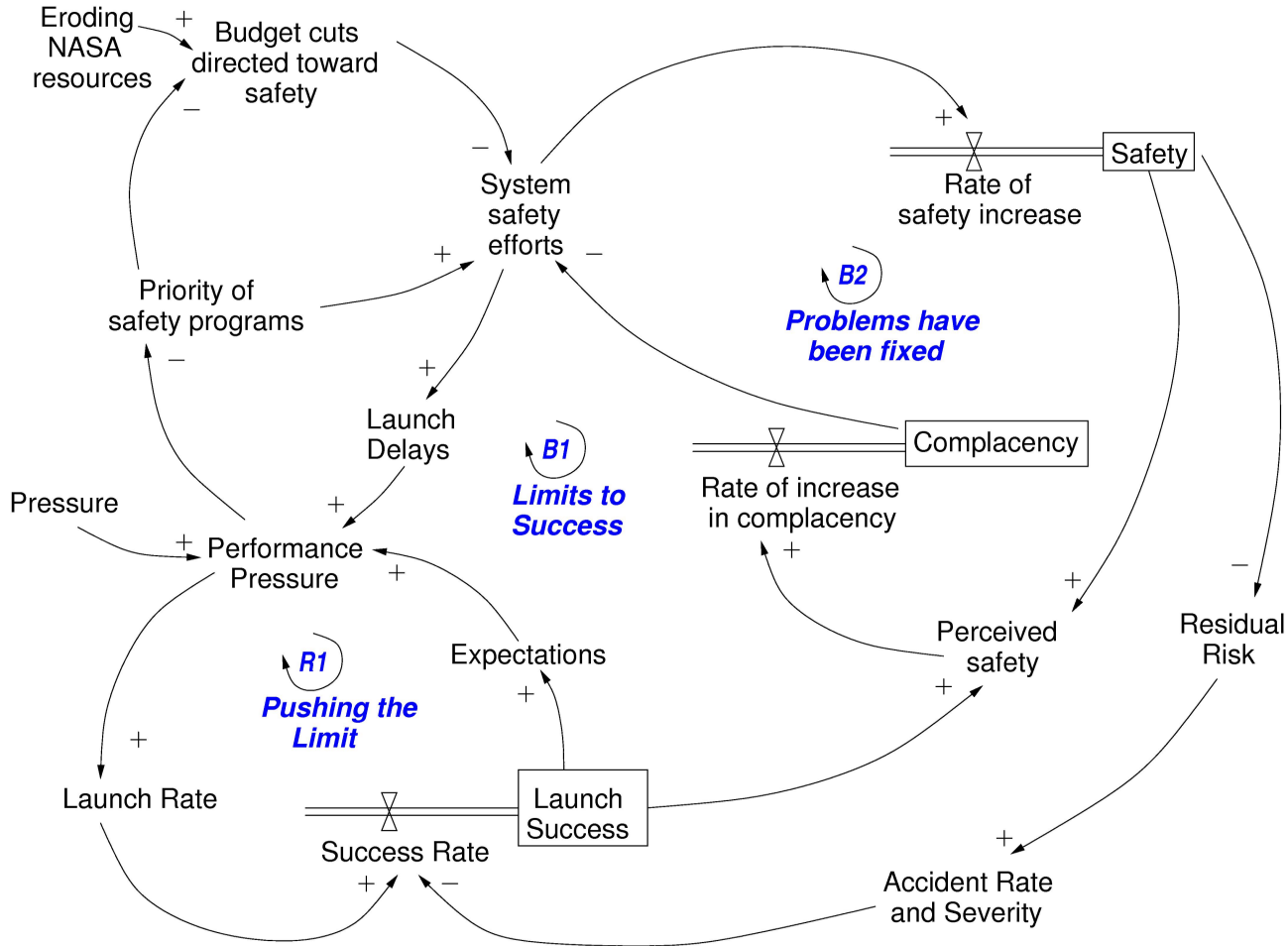
A process for measuring and tracking outcomes



RCA: Tree diagram



Dynamic systems modeling



**Example:
Columbia Space Shuttle Accident
[Leveson 2007]**



Aalto University

2. Human Error

Definition: Human error

- An inappropriate or undesirable human decision or behavior that reduces or has the potential to reduce effectiveness, safety, or system performance
- A human action/decision that exceeds system tolerances
- *”An action is taken that was ‘not intended by the actor; not desired by a set of rules or an external observer; or that led the task or system outside its acceptable limits’”*

(Senders & Moray, 1991, p. 25 as cited in Proctor & van Zandt, 1994, p. 43).

Several decades of research



Errors observed with new technology

Mode Error – user thought system was in one mode when it was actually in another.

Getting Lost – Users get lost in display architectures.
Difficulty in finding the right screen or data set.

Not Coordinating Data Entries – poor coordination between multiple users inputting data into the same system.

Overload – system use drains attention resources from other equally important tasks.

Data Overload –users forced to sort through a large amount of data produced by the system in order to determine the true nature of the situation.

Not Noticing Changes – digital displays used to communicate system changes or trends.

Automation Surprises – system automation did something user did not expect or anticipate.

Taxonomy 1/3: Stages of human error

1. Activation/detection of system state signal
2. Observation and data collection
3. Identification of system state
4. Interpretation of situation
5. Definition of objectives
6. Evaluation of alternative strategies
7. Procedure selection
8. Procedure execution



Taxonomy 2/3: Action errors

- **Intrusion** – entering a dangerous area / location
- **Commission** – performing an act incorrectly
- **Omission** – failure to do something
- **Reversal** – trying to stop or undo a task already initiated
- **Misordering** – task or set of task performed in the wrong sequence
- **Mistiming** – person fails to perform the action within the time allotted

Taxonomy 3/3:

Memory failures

Losing ones place

Forgetting intentions

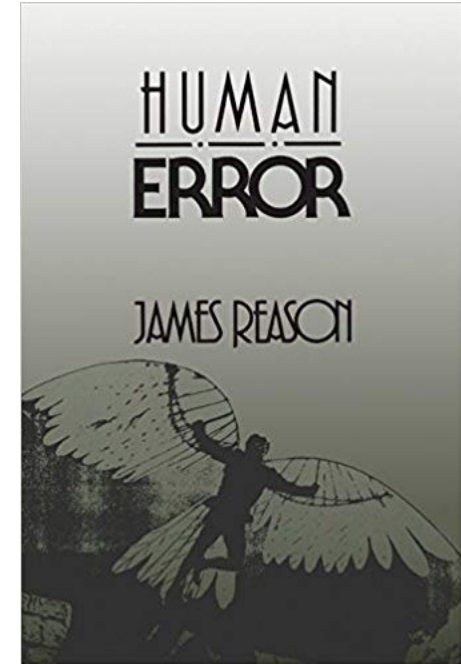
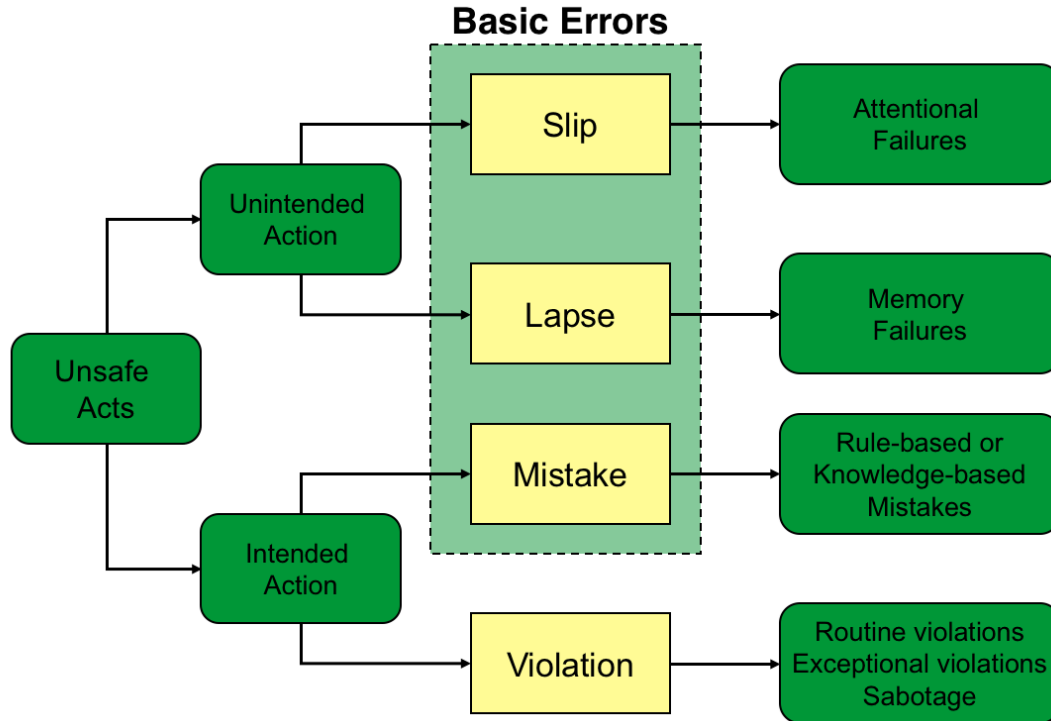
Application of a bad rule

“I’ m in a public space in view of many people, therefore I won’ t be robbed.”

Misapplication of a good rule

“A patient on chronic medication became concerned about addiction and therefore deliberately stop taking the drug for a period each year even though the drug in question was not addictive.”

James Reason's taxonomy





Aalto University

Rasmussen's SRK

Skills, Rules, Knowledge



Rasmussen's SRK: Skills, Rules, Knowledge

Example from power plant operation

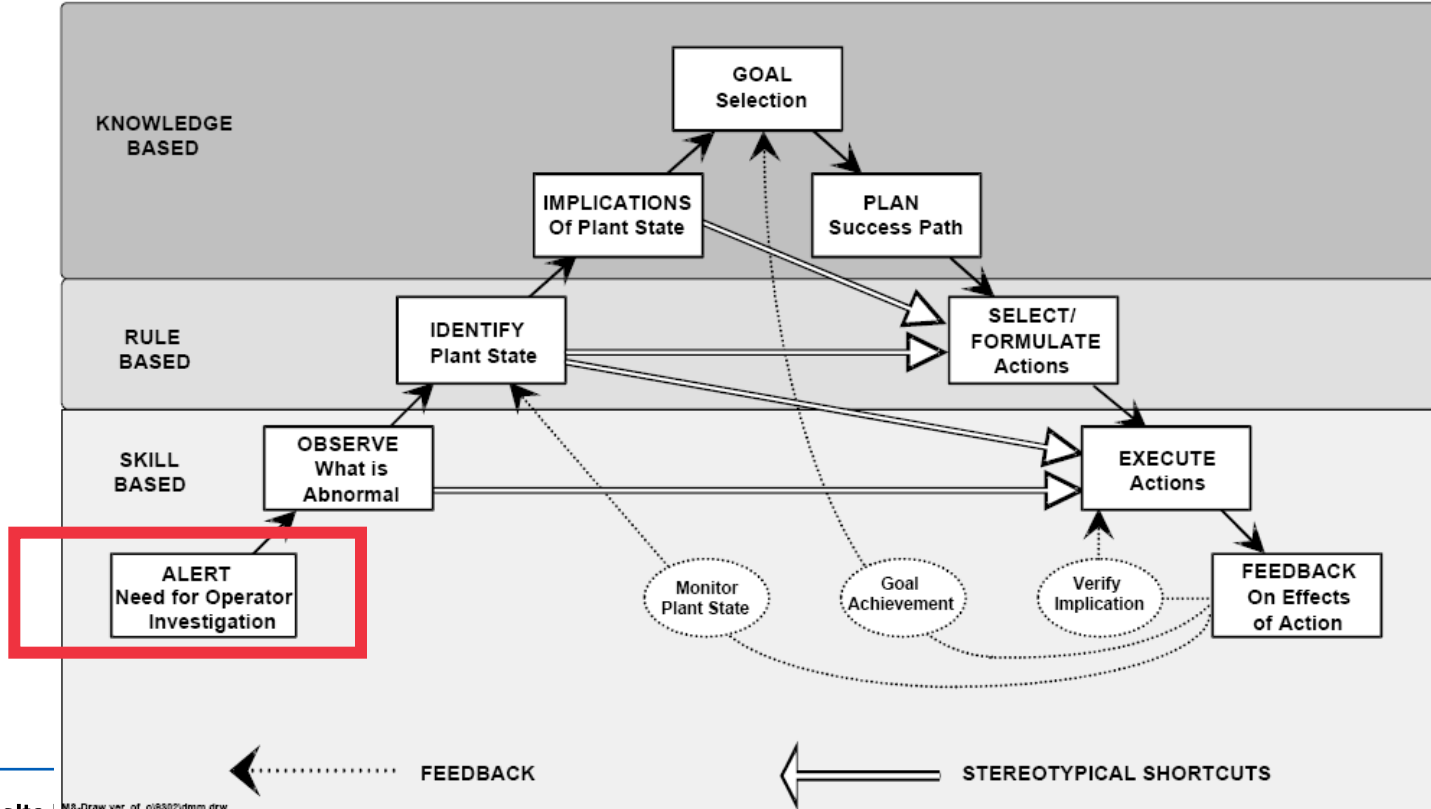


Figure 5: Decision-Making Model (adapted from Rasmussen) including Feedback



Skills, Rules, Knowledge (SRK)

Q: What are the skills, rules, and knowledge you need to log in?



Username

> [Target site's privacy policy](#)

Password

> [About this service](#)

Login

[Revoke attribute release approval](#)

A?

Aalto University

Accident prevention by standards

**Good to
know**



Use-Related Risks: Infusion Pumps

Hazard (samples)	Corresponding Risk(s) to Health	Use-Related Cause(s) (samples)
Infusion stopped prematurely	<ul style="list-style-type: none"> • Underdose • Delay of therapy 	<p>The user forgets to resume the pump after suspending it</p> <p>User is unaware of battery capacity</p>
The user fails to detect or understand pump notifications	<ul style="list-style-type: none"> • Overdose • Underdose • Delay of therapy • Incorrect therapy 	<p>Background noise or nuisance alarms cause user to fail to detect/ignore them</p> <p>User muffles pump's speaker/audio, either intentionally or unintentionally</p>
Wrong medication or concentration is delivered	<ul style="list-style-type: none"> • Incorrect therapy • Delay of therapy 	<p>User selects and sets up pump with incorrect medication or concentration</p> <p>Medication is correct but user selects incorrect concentration or delivery rate</p>

Excerpt from requirements for infusion



Technical Reports (CIS)

Departments

2-6-2009

Generic Infusion Pump Hazard Requirements Version 1.0

David E. Arney
University of Pennsylvania

Raoul Jetley
Office of Science and Engineering Laboratories, Food and Drug Administration

Paul Jones
Office of Science and Engineering Laboratories, Food and Drug Administration

Insup Lee
University of Pennsylvania, lee@cis.upenn.edu

Arnab Ray
Fraunhofer Center for Experimental Software Engineering

See next page for additional authors

Follow this and additional works at: <http://repository.upenn.edu>
Part of the [Numerical Analysis and Scientific Computing](#)

Recommended Citation

David E. Arney, Raoul Jetley, Paul Jones, Insup Lee, Arnab Ray, Oleg Sokolsky, and Safety Requirements Version 1.0, February 2009.

University of Pennsylvania Department of Computer and Information Science Technical Reports

This paper is posted at ScholarlyCommons. http://repository.upenn.edu/cis_reports/893
For more information, please contact libraryrepository@pobox.upenn.edu.

2 User Interface

2.1 Resistance to tampering and accidents

- 2.1.1 To avoid accidental tampering of the pumps settings such as the flow rate/VTBI, at least two steps should be required to change the settings.
- 2.1.2 Changing settings, such as the patients weight or infusion duration, while the pump is infusing, should either not be allowed, or at least require confirmation.
- 2.1.3 The administration set should be designed to prevent compromising patient safety or cause an unacceptable flow error.
- 2.1.4 There shall be no multiple-key legal values. That is, there should be no legal inputs that require multiple keys to be pressed simultaneously.
- 2.1.5 If the numeric keypad cover is broken or unlocked during infusion, the pump should issue an alarm to indicate illegal tampering.

2.2 User input

- 2.2.1 If the pump is in a state where user input is required, the pump shall issue periodic alerts/indications every 15 minutes till the required input is provided.
- 2.2.2 The pump shall issue an alert if paused for more than x minutes
- 2.2.3 Clearing of the pump settings and resetting of the pump shall require confirmation.
- 2.2.4 If the pump is idle for 5 minutes while programming a dose setting, the pump shall issue an alert to indicate that the user needs to finish programming/start infusion
- 2.2.5 If the pump is idle for more than 10 minutes while programming a dose setting, the pump shall issue an alarm and clear the dose parameters defined.
- 2.2.6 Each time the pump is turned on, the system should require the user to indicate whether the pump is being used on a new patient and to select (or confirm, if not a new patient) the current clinical location.
- 2.2.7 For a multi-channel pump:
 - 2.2.7.1 The pump should display the drug/solution name and dose being infused by each channel.
 - 2.2.7.2 The system should trigger an alert if the same drug or solution is programmed on more than one channel. It should be possible to override the alert if the programming is intentional.



Aalto University

3. Task Analysis

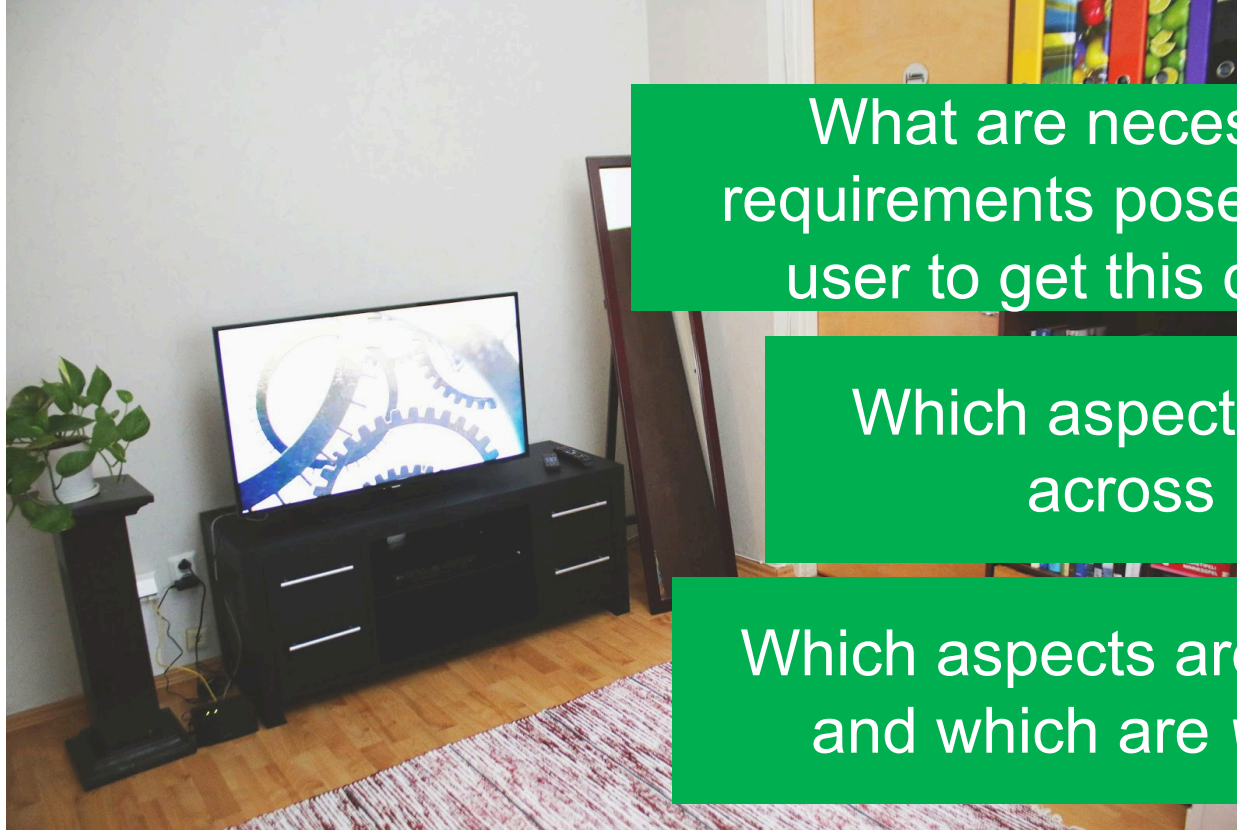


Warm up: Describe (verbally) how to turn on the television

What are necessary requirements posed to the user to get this done?

Which aspects might differ across users?

Which aspects are *invariant* and which are *variant*?





A person wearing a blue and white plaid shirt is using a power drill on a wooden table. The person's left hand is on the drill's handle, and their right hand is holding a black plastic component. A black watch with a white face is visible on their left wrist. The background is a blurred indoor setting.

What do users EXPECT
from the technology?

How may they TRY to use
it?

What is REQUIRED of the
user?

What types of errors or
mistakes may they do?

HTA: Learning objectives

The idea: Decomposition of tasks

- Sequential, hierarchical, probabilistic aspects

Know that empirical methods are used to obtain task descriptions

Hierarchical task analysis (HTA)



Aalto University

**Task analysis decomposes
user behavior to recover the
variant and invariant aspects
of interaction**

Even the most mundane of our activities involve tasks

AMERICAN TIME USE

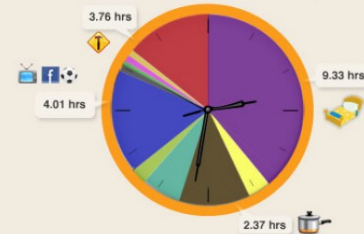
Did you know that if you work an 8 hour day, you're not the norm? Think your hour or two on Facebook or emailing every day is pretty typical? Think again. The U.S. Department of Labor recently did a survey of how the average American spends their day, the results of which you may find quite surprising.

The Average Employed American's Weekday

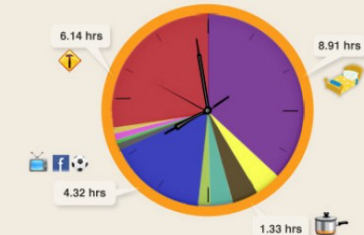


The categories in this infographic refer to an individual's main activity. Other activities done simultaneously are not included. All major activity categories include related travel time. "The Average Employed American" in this graphic has children at home. Statistics are 2008 Annual Averages provided by U.S. Dept. of Labor: <http://www.bls.gov/news.release/at.us.nr0.htm>

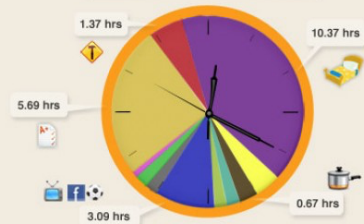
Women Ages 35-44 Years Old



Men Ages 35-44 Years Old



Boys & Girls Ages 15-19 Years Old



Claim: Everything we do with technology entails some “task”

Goal-orientedness is a defining feature of technology use





Design may succeed or fail in guiding the user through the task

Task performance as a sequence



- Step 1: **Find** vending machine room
- Step 2: **Identify** soda vending machines (SVMs) in vending machine room
- Step 3: **Search** SVM 1 for desired soda brand (X)
- Step 4: **Search** SVM 2 for desired soda brand (X)
- Step 5: **Search** SVM 3 for desired soda brand (X)
- Step 6: **Search** SVM 3 for cost of Brand X
- Step 7: **Search** SVM 3 for money slot
 - Does it accept quarters only?
 - Does it accept dollars and quarters?
- Step 8: **Find** change in pocket
- Step 9: **Get** change from pocket
- Step 10: **Examine** change for quarters
- Step 11: **Get** wallet from pocket
- Step 12: **Examine** bills in wallet for \$1.00 bills
- Step 13: **Get** one \$1.00 bill from wallet
- Step 14: **Put** wallet in pocket
- Step 15: **Put** unneeded change in pocket
- Step 16: **Insert** money into SVM 3
- Step 17: **Select** Brand X on SVM 3 button array
- Step 18: **Get** soda
- Step 19: **Enjoy** a refreshing beverage

A

Figure 11.2 Example of a task description for the task of buying a beverage from a vending machine.

Hierarchical task analysis (HTA)

An **analytical** method developed in human factors but adopted widely in human-computer interaction and interaction design

- Over 20 different TA methods used in human factors for decades

A powerful, unifying **decomposition** of human activities:

- **Hierarchy** (task B is a subtask of task A)
- **Sequence** (task A follows task B)
- **Choice** (tasks A and B are alternative)
- **Parallelism** (task A is done at the same time as task B)



Many formalisms

Task Model Relationships

	AMBOSS	ANSI/CEA	CTT	Diane +	GOMS	GTA	HTA	TKS	TOOD	UsiXML	Relevance
Decomposition	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Hierarchy	Must
Sequence	Seq	+ Ordered = true, information passing (Postcondition)	Enabling, enabling with information passing	Ordered sequence	Sequence	Seq	Fixed sequence	Sequence	Sequence	Enabling, enabling with information passing	Must
Iteration	X	+ MinOccurs+ MaxOccurs	Iteration, finite iteration	Loop	+ Loop (If, then, else)	X	+ Stop rules	X	X	Iteration, finite iteration	Should
Choice	ALT	+ Precondition	Choice	Required choice, free choice	+ Or (If, then, else)	Or	Selective rule	Or	Choice	Deterministic choice, undeterministic choice, inclusive choice	Should
Optionality	Barrier	MinOccurs/MaxOccurs	Optional	Optional	Optional (If, then, else)	Start condition	X	X	X	Optional	Should
Interruption	X	X	Suspend- resume, disabling	X	Interruption (If, then, else)	Stop condition	Stop rules	X	Interruption	Suspend- resume, disabling, disabling with information passing	Should
Concurrency	SER	Ordered = false	Concurrent, concurrent communicating tasks, independence	unordered sequence	Concurrency (If, then, else)	X	Selective rule	X	Concurrency	Independent concurrency, concurrency with information passing, order independence	Should
Cooperation	Precondition	X	Cooperative	X	X	Cooperation	Teamwork	Collaboration(FKS extension)	Collaboration	Cooperation	Should
Parallel	PAR, SIM	X	X	Parallel	X	And	Dual task (time sharing)	And	Simultaneity	parallelSplit (process model)	Should

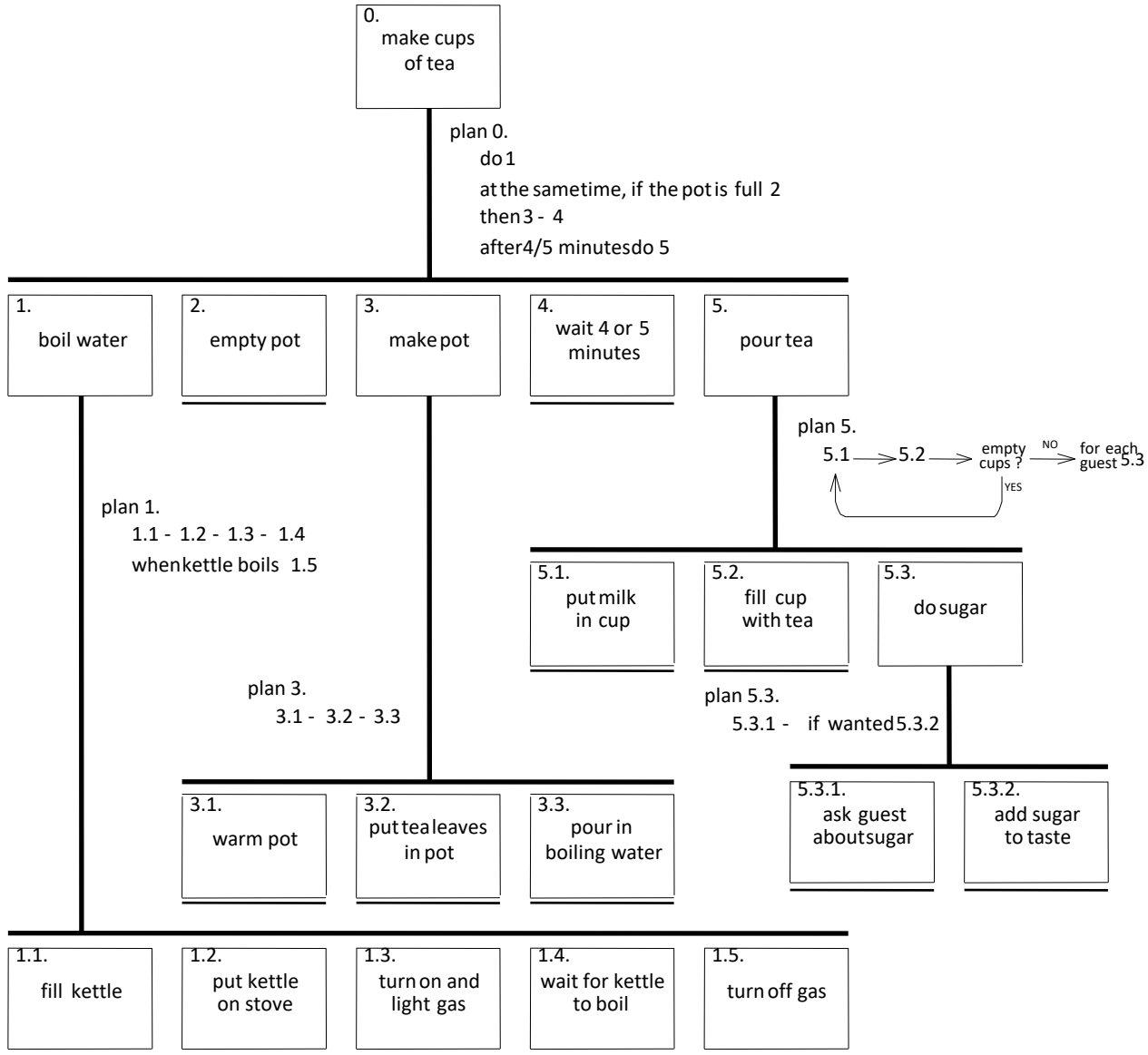


Hierarchy (task B is a subtask of task A)

Sequence (task A follows task B)

Choice (tasks A and B are alternative)

Parallelism (task A is done at the same time as task B)



Empirical method for obtaining HTAs

Iteration and validation with stakeholders

Annett 2004

Steps in Hierarchical Task Analysis
according to Annett 2004:

1. Decide the purpose(s) of the analysis
2. Get agreement between stakeholders on the definition of task goals and criterion measures
3. Identify sources of task information and select means of data acquisition
4. Acquire data and draft decomposition table/diagram
5. Re-check validity of decomposition with stakeholders
6. Identify significant operations in light of purpose of analysis
7. Generate and, if possible, test hypotheses concerning factors affecting learning and performance.

Basic concepts

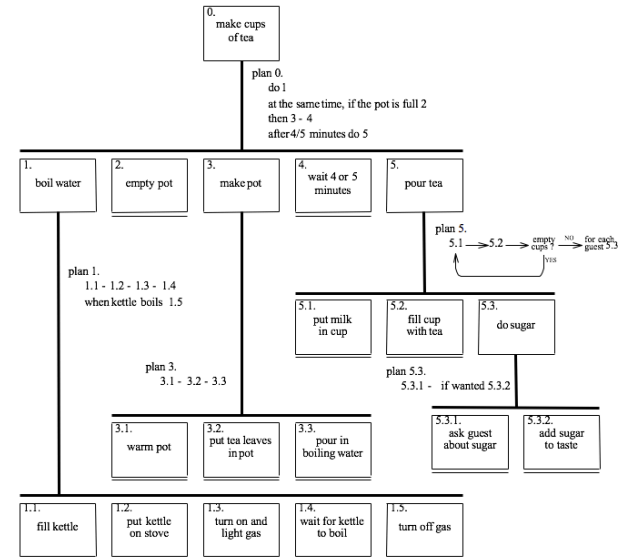
Each **subtask** is specified by

- a **goal**,
- **conditions** for the goal to be activated,
- **actions** required to attain the goal, and
- **feedback** (optionally) indicating success.

Plans tie together subtasks and superordinate tasks



Draw an HTA diagram for measuring fever. Raise hand when ready





Why bother “analyzing” tasks?



Predicting and minimizing errors

Task step	Error probability	Error consequence	Criticality of error
1: Find closest vending machine room	Low	No soda or delay in getting soda plus extra effort	High
2: Identify soda vending machines (SVMs) in vending machine room	Low	No soda or delay in getting soda plus extra effort	High
3: Search SVM 1 for desired soda brand (X)	Low	Miss soda on SVM 1	Low
4: Search SVM 2 for desired soda brand (X)	Low	Miss soda on SVM 2	Low
5: Search SVM 3 for desired soda brand (X)	Low	Miss soda on SVM 3	Low
6: Search SVM 3 for cost of Brand X	Low	Possibility of insufficient funds	High
7: Search SVM 3 for money slot <ul style="list-style-type: none"> • Quarters only? • Dollars and quarters? 		Possibility of insufficient funds	High
8: Find change in pocket	Low	Possibility of insufficient funds	High
9: Get change from pocket	Medium	1. Repeat step 9 2. Pick up change from floor	Medium
10: Examine change for quarters	Low	Possibility of insufficient funds	High
11: Get wallet from pocket	Low	1. Repeat step 11 2. Pick up wallet from floor	Medium
12: Examine bills in wallet for \$1.00 bills	Medium	1. Repeat step 12 2. No soda	Medium
13: Get one \$1.00 bill from wallet	Low	1. Repeat step 13 2. Pick up \$1.00 bill from floor	Medium
14: Put wallet in pocket	Low	1. Repeat step 11 2. Pick up wallet from floor	Medium
15: Put unneeded change in pocket	Medium	1. Repeat step 15 2. Pick up change from floor	Medium
16: Insert money into SVM 3	Medium	1. Repeat step 16 2. Pick up change and/or \$1.00 bill from floor	Medium
17: Select Brand X on SVM 3 button array	Medium	Wrong soda	High
18: Get soda	Low	1. Repeat step 18 2. Pick up soda from floor	Medium
19: Enjoy a refreshing beverage	Low	Clean soda off front of shorts	High

Figure 11.3 Example of hierarchical task analysis for the task of buying a beverage from a vending machine.

Expose and minimize complexity

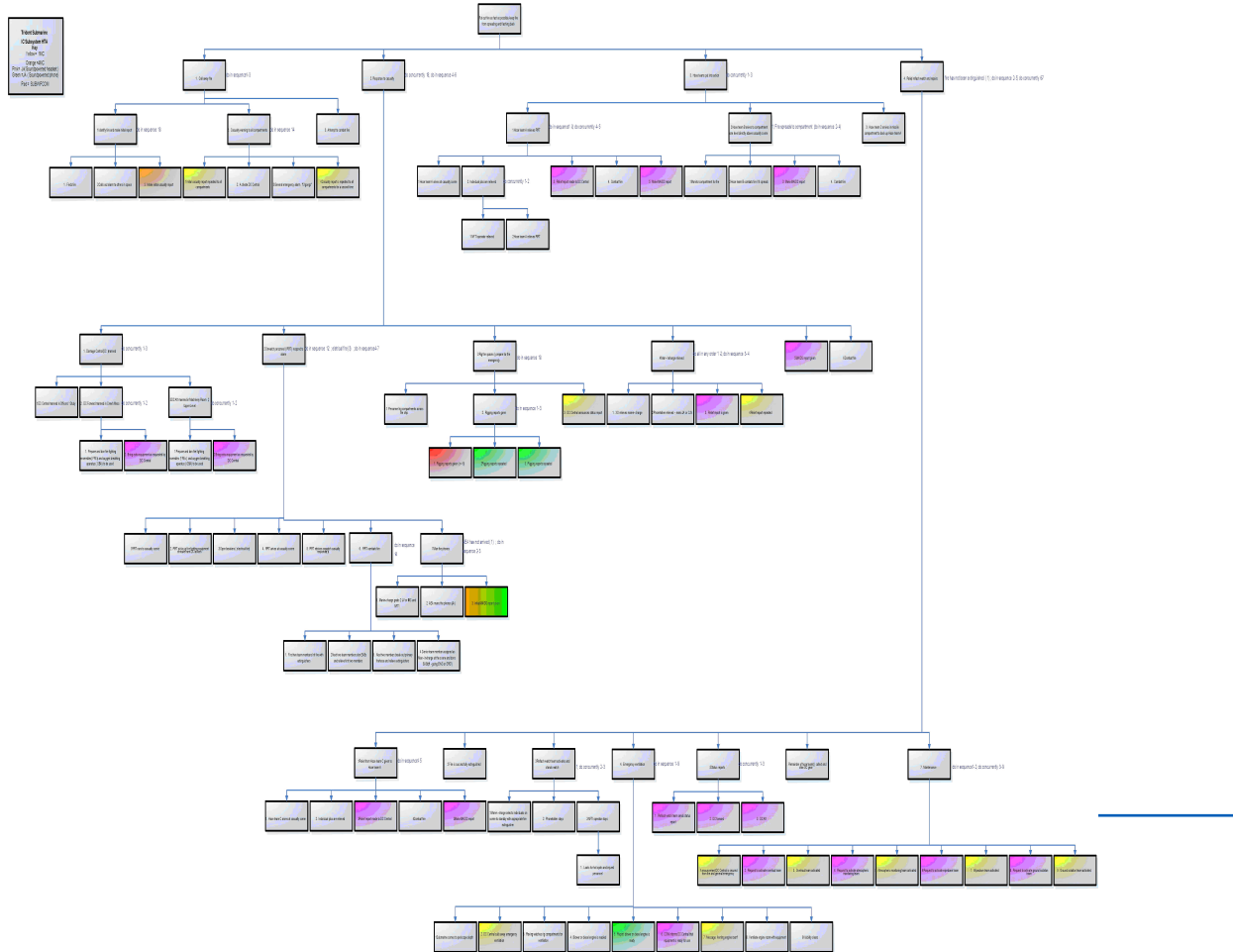


- Step 1: **Find** vending machine room
- Step 2: **Identify** soda vending machines (SVMs) in vending machine room
- Step 3: **Search** SVM 1 for desired soda brand (X)
- Step 4: **Search** SVM 2 for desired soda brand (X)
- Step 5: **Search** SVM 3 for desired soda brand (X)
- Step 6: **Search** SVM 3 for cost of Brand X
- Step 7: **Search** SVM 3 for money slot
 - Does it accept quarters only?
 - Does it accept dollars and quarters?
- Step 8: **Find** change in pocket
- Step 9: **Get** change from pocket
- Step 10: **Examine** change for quarters
- Step 11: **Get** wallet from pocket
- Step 12: **Examine** bills in wallet for \$1.00 bills
- Step 13: **Get** one \$1.00 bill from wallet
- Step 14: **Put** wallet in pocket
- Step 15: **Put** unneeded change in pocket
- Step 16: **Insert** money into SVM 3
- Step 17: **Select** Brand X on SVM 3 button array
- Step 18: **Get** soda
- Step 19: **Enjoy** a refreshing beverage

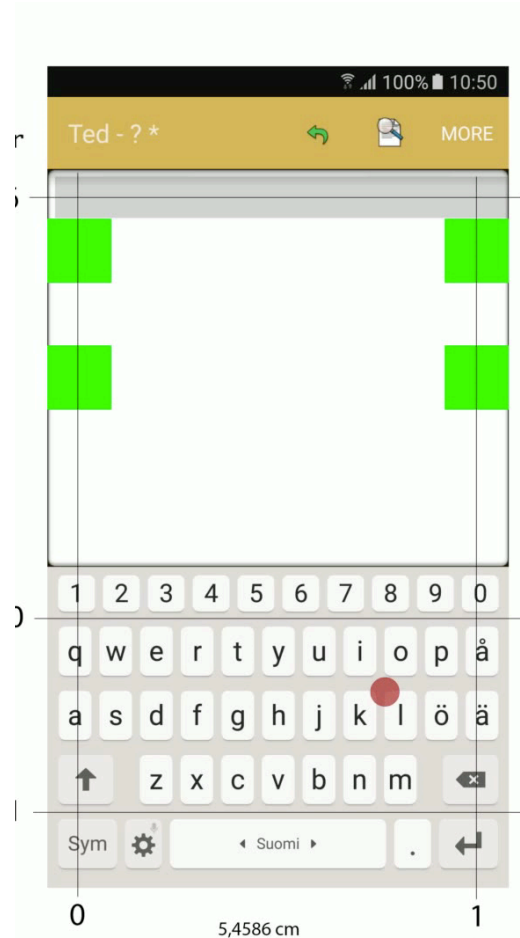
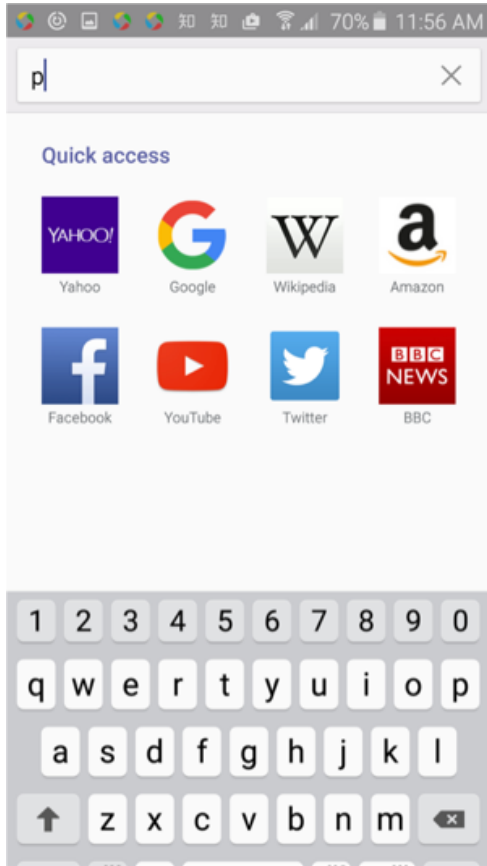
Figure 11.2 Example of a task description for the task of buying a beverage from a vending machine.



Expose needs for training



Even very “small” tasks have structure



Even “waiting” is a task

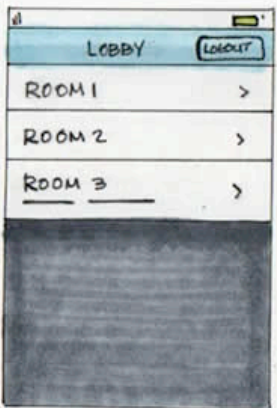
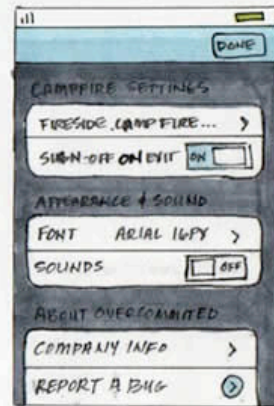
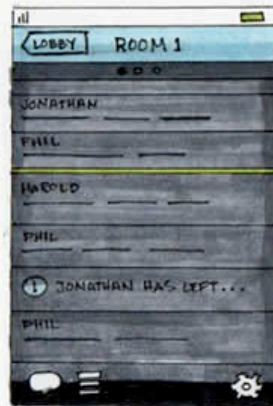
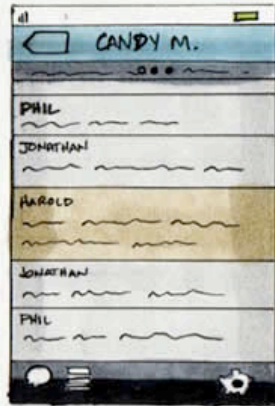


Tasks are the basis of user-centered design

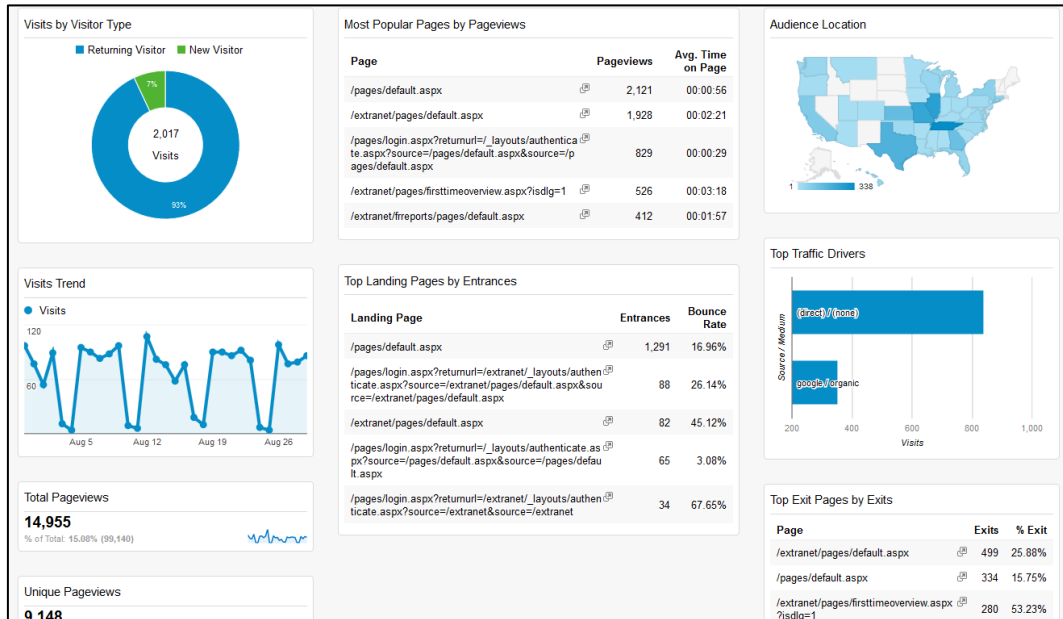
Tasks define **measurable objectives** for design and evaluation.



Sketching and prototyping often centers on users' tasks



User data is meaningless unless you understand what people do



Google Analytics



Aalto University

Automation and Human Error



Q: What should a machine vs. human do?

**(replacement) trivializes
the effects of automation!**

Levels of automation

TABLE 2.1: A Scale of Degrees of Automation

1. The computer offers no assistance; the human must do it all.
 2. The computer suggests alternative ways to do the task.
 3. The computer selects one way to do the task and
 4. executes that suggestion if the human approves, or
 5. allows the human a restricted time to veto before automatic execution, or
 6. executes the suggestion automatically, then necessarily informs the human, or
 7. executes the suggestion automatically, then informs the human only if asked.
 8. The computer selects the method, executes the task, and ignores the human.
-























Q: Automation levels: Setting the temperature of an industrial freezer?



TABLE 2.1: A Scale of Degrees of Automation

-
1. The computer offers no assistance; the human must do it all.
 2. The computer suggests alternative ways to do the task.
 3. The computer selects one way to do the task and
 4. executes that suggestion if the human approves, or
 5. allows the human a restricted time to veto before automatic execution, or
 6. executes the suggestion automatically, then necessarily informs the human, or
 7. executes the suggestion automatically, then informs the human only if asked.
 8. The computer selects the method, executes the task, and ignores the human.
-

There are Six Levels of Automation

Level	Name	Who is Driving?	Who is Monitoring?	Who Intervenes?
0	No Automation			
1	Driver Assist			
2	Partial Automation			
3	Conditional Automation			
4	High Automation			
5	Full Automation			

Source: Adapted from NHTSA and SAE J3016

Case: Self-driving cars

Studies of autopilot

Boeing 727



Ironies of automation

”Even highly automated systems, such as electric power networks, need human beings... one can draw the paradoxical conclusion that automated systems still are man-machine systems, for which both technical and human factors are important”

Lisa Bainbridge 1984

Known consequences of bad automation

Bainbridge's "Ironies of automation"

1. misunderstanding or missing feedback
2. misunderstanding operating logic
3. overreliance
4. lack of trust
5. mixed-initiative conflict
6. alienation
7. deskilling
8. denying responsibility

Immediate causes of human-automation failures

Brittle automation: Only responds to a narrow set of situations

Combination with information outside the system

Unavailable warning about reaching the limits of automation

Insufficient feedback about the state of the automation

Inadequate interpretation of device state by operator

Mode confusion: Inability to keep track of and predict device state

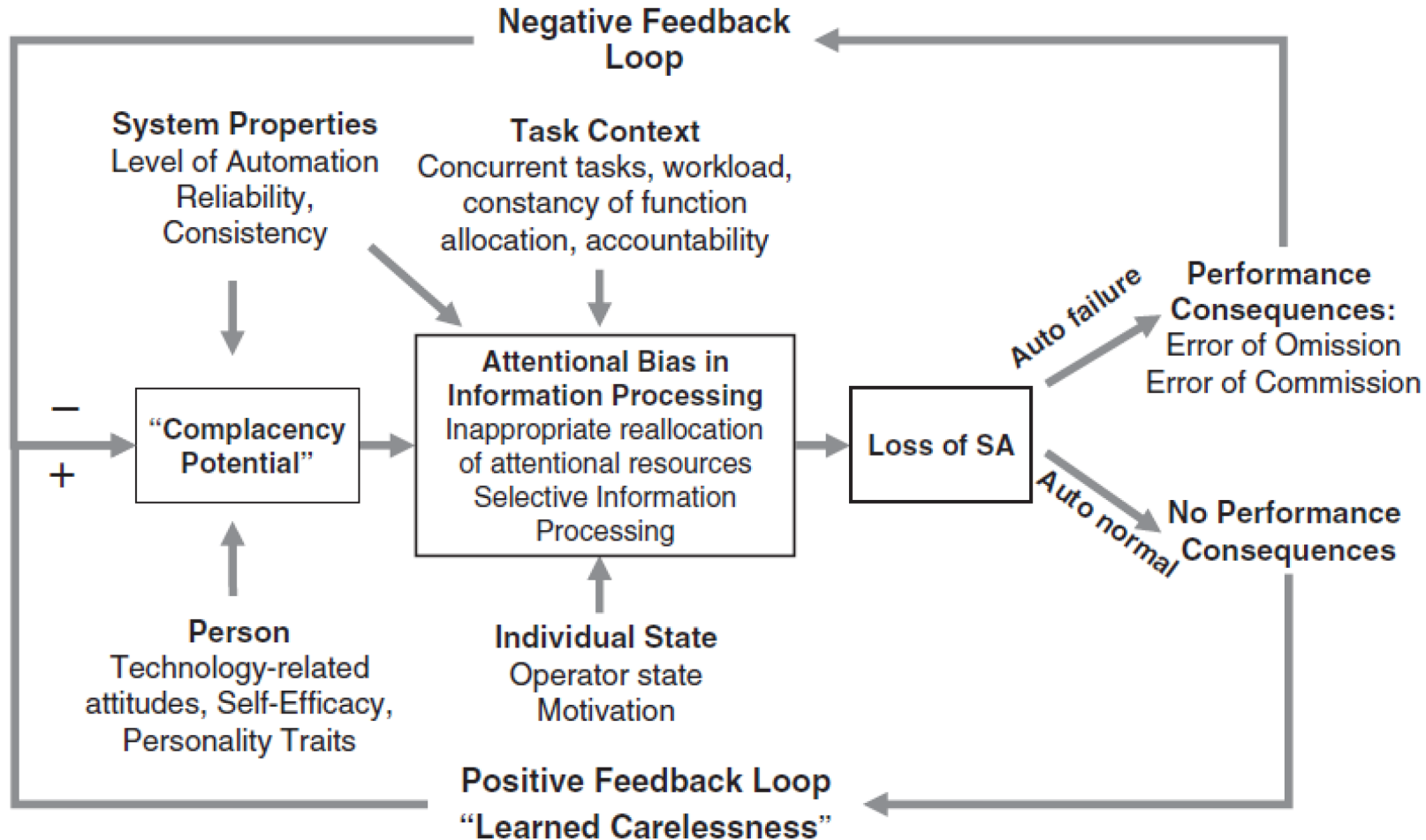
Overreliance on automation, habit-formation

Deskilling

Loss of vigilance

Learned carelessness

SA = situation awareness



Asiana Flight 2013

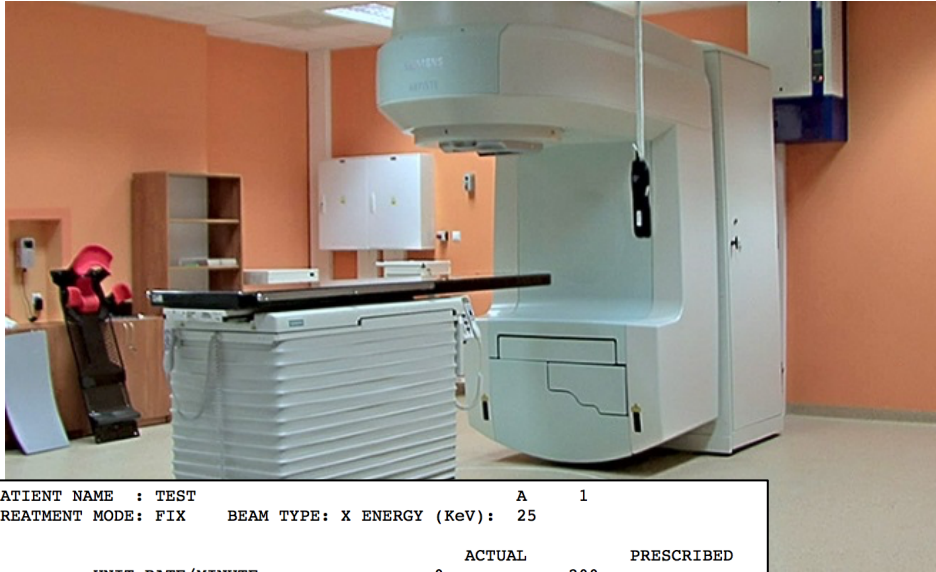


Air France Flight 447 2009

“The official cause of the accident was the freezing of the pitot tubes which caused the autopilot to disconnect. The aircraft switched from normal law to alternate law with no stall protection on control inputs. The misdiagnosis of the situation led to the pilot demanding full nose up.”



Therac-25 Medical Accelerator - 1985-7



“An operator involved in an overdose accident testified that she had become insensitive to machine malfunctions. Malfunction messages were commonplace, most did not involve patient safety. Service technicians would fix the problems or the hospital physicist would realign the machine and make it operable again.”

```
PATIENT NAME : TEST           A      1
TREATMENT MODE: FIX    BEAM TYPE: X ENERGY (KeV): 25

UNIT RATE/MINUTE           0      200
MONITOR UNITS              50    50    200
TIME (MIN)                 0.27 1.00

GANTRY ROTATION (DEG)      0.0      0 VERIFIED
COLLIMATOR ROTATION (DEG) 359.2    359 VERIFIED
COLLIMATOR X (CM)         14.2    14.3 VERIFIED
COLLIMATOR Y (CM)         27.2    27.3 VERIFIED
WEDGE NUMBER              1      1 VERIFIED
ACCESSORY NUMBER          0      0 VERIFIED

DATE : 84-OCT-26  SYSTEM: BEAM READY  OP.MODE: TREAT  AUTO
TIME : 12:55. 8  TREAT : TREAT PAUSE  X-RAY      173777
OPR ID: T25VO2-RO3 REASON: OPERATOR  COMMAND:
```

Figure A. Operator interface screen layout.

Grounding of Royal Majesty - 1995



Checklists and SOPs



Checklist for Anaesthetic Equipment 2012

AAGBI Safety Guideline



Checks at the start of every operating session

Do not use this equipment unless you have been trained

Check self-inflating bag available

Perform manufacturer's (automatic) machine check

Power supply

- Plugged in
- Switched on
- Back-up battery charged

Gas supplies and suction

- Gas and vacuum pipelines – 'tug test'
- Cylinders filled and turned off
- Flowmeters working (if applicable)
- Hypoxic guard working
- Oxygen flush working
- Suction clean and working

Breathing system

- Whole system patent and leak free using 'two-bag' test
- Vaporisers – fitted correctly, filled, leak free, plugged in (if necessary)
- Soda lime - colour checked
- Alternative systems (Bain, T-piece) – checked
- Correct gas outlet selected

Ventilator

- Working and configured correctly

Scavenging

- Working and configured correctly

Monitors

- Working and configured correctly
- Alarms limits and volumes set

Airway equipment

- Full range required, working, with spares

RECORD THIS CHECK IN THE PATIENT RECORD

Don't Forget!

- Self-inflating bag
- Common gas outlet
- Difficult airway equipment
- Resuscitation equipment
- TIVA and/or other infusion equipment

This guideline is not a standard of medical care. The ultimate judgement with regard to a particular clinical procedure or treatment plan must be made by the clinician in the light of the clinical data presented and the diagnostic and treatment options available.

© The Association of Anaesthetists of Great Britain & Ireland 2012

Tesla autopilot fails (no warnings)



TABLE 2.2: Some Criteria of Human-Centered Automation (and Reasons to Question Them)

1. Allocate to the human the tasks best suited to the human, and allocate to the automation the tasks best suited to it. (Unfortunately, there is no consensus on how to do this; nor is the allocation policy necessarily fixed, but may depend on context.)
2. Keep the human operator in the decision-and-control loop. (This is good only for intermediate-bandwidth tasks. The human is too slow for high bandwidth and may fall asleep if bandwidth is too low.)
3. Maintain the human operator as the final authority over the automation. (Humans are poor monitors, and in some decisions it is better not to trust them; they are also poor decision makers when under time pressure and in complex situations.)
4. Make the human operator's job easier, more enjoyable, or more satisfying through friendly automation. (Operator ease, enjoyment, and satisfaction may be less important than system performance.)

5. Empower or enhance the human operator to the greatest extent possible through automation. (Power corrupts.)
 6. Support trust by the human operator. (The human may come to overtrust the system.)
 7. Give the operator computer-based advice about everything he or she should want to know. (The amount and complexity of information is likely to overwhelm the operator at exactly the worst time.)
 8. Engineer the automation to reduce human error and minimize response variability. (A built-in margin for human error and experimentation helps the human learn and not become a robot; see Rasmussen, Pedersen, & Goodstein, 1995.)
 9. Make the operator a supervisor of subordinate automatic control systems. (Sometimes straight manual control is better than supervisory control.)
 10. Achieve the best combination of human and automatic control, where best is defined by explicit system objectives. (Rarely does a mathematical objective function exist.)
-

Expertise and adaptability as the rule

Assign roles based on information processing requirements

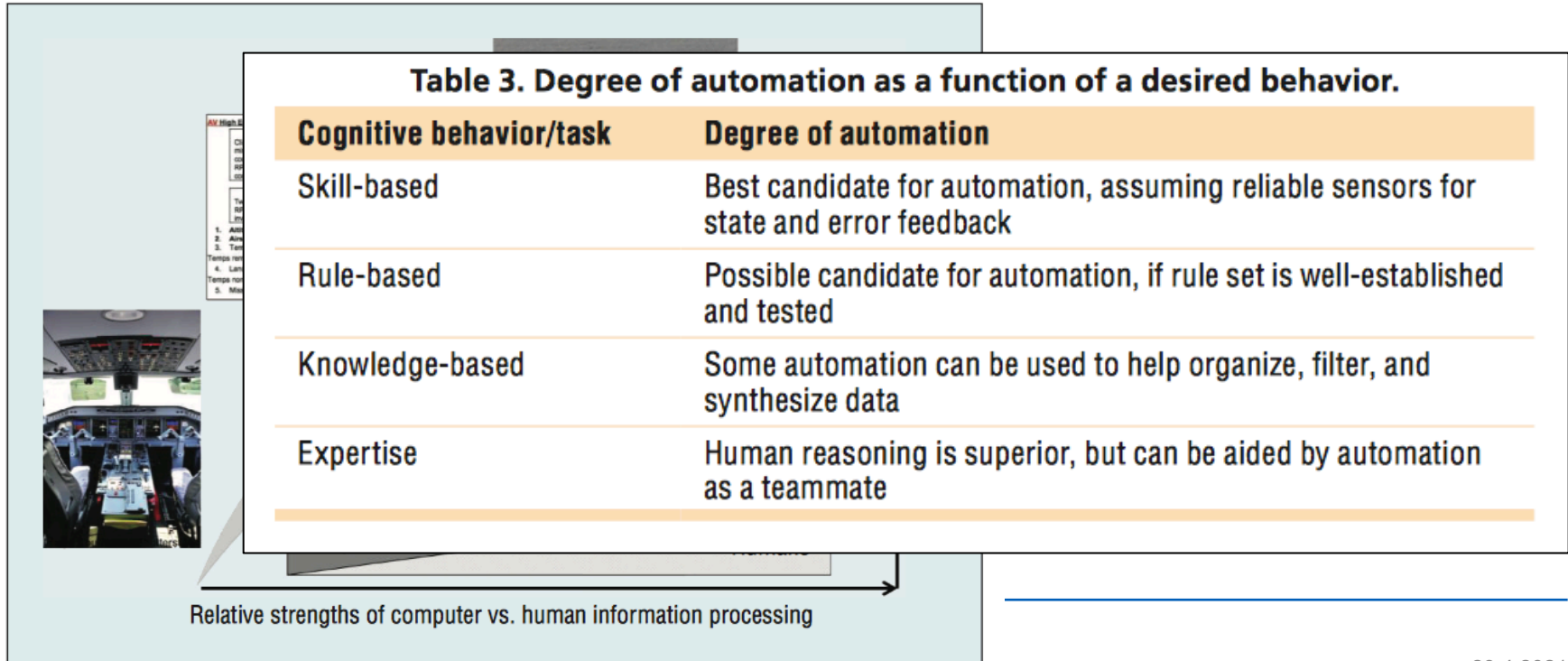
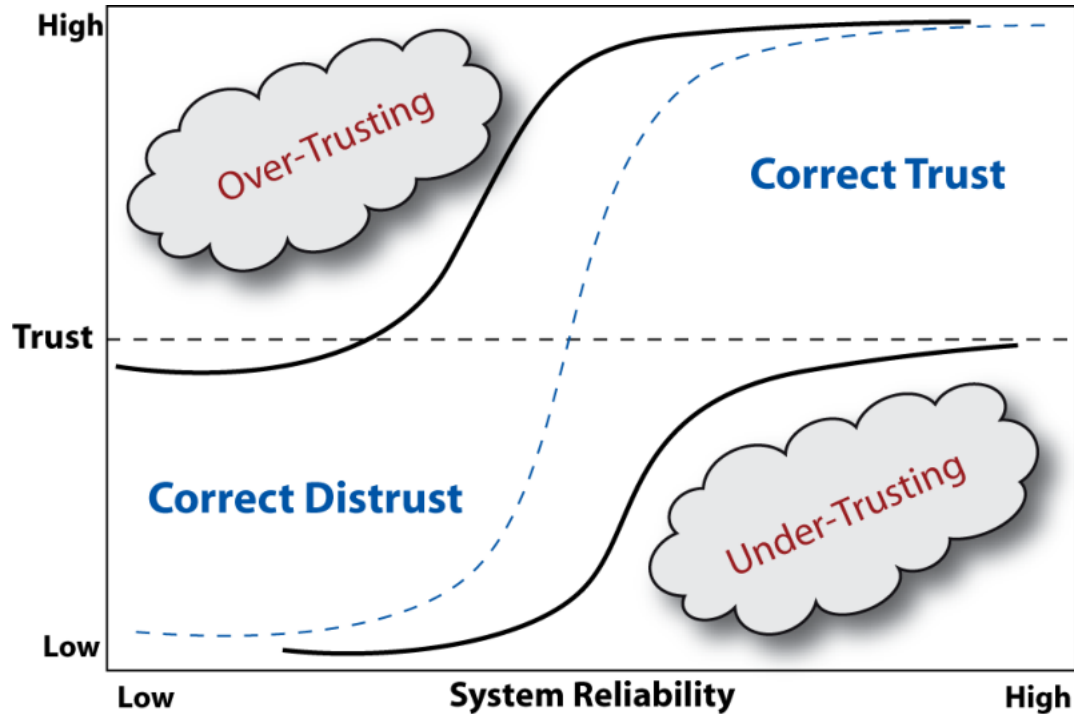


Figure 2. Role allocation for information processing behaviors (skill, rule, knowledge, and expertise) and the relationship to uncertainty.

Calibration of trust



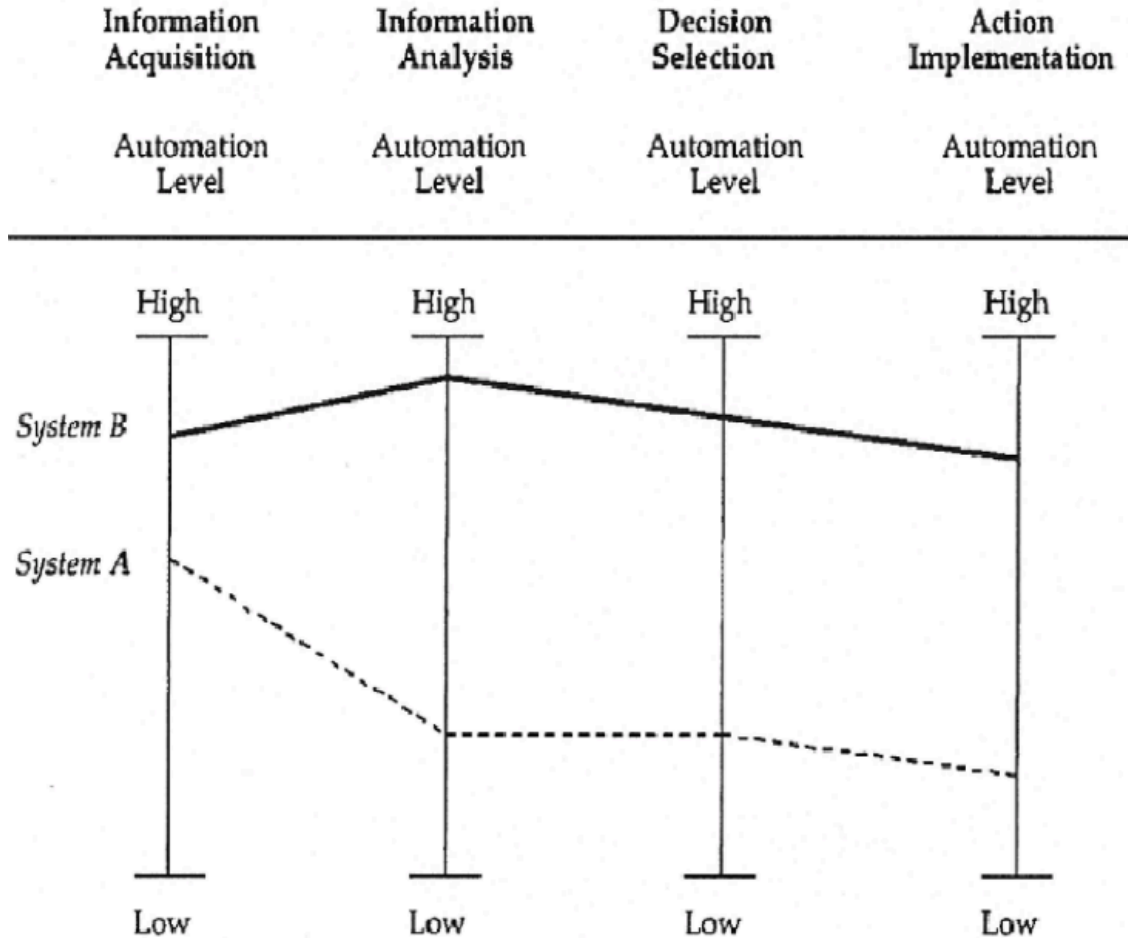
Levels of automation theory: Revisited

TABLE 2.1: A Scale of Degrees of Automation

1. The computer offers no assistance; the human must do it all.
 2. The computer suggests alternative ways to do the task.
 3. The computer selects one way to do the task and
 4. executes that suggestion if the human approves, or
 5. allows the human a restricted time to veto before automatic execution, or
 6. executes the suggestion automatically, then necessarily informs the human, or
 7. executes the suggestion automatically, then informs the human only if asked.
 8. The computer selects the method, executes the task, and ignores the human.
-

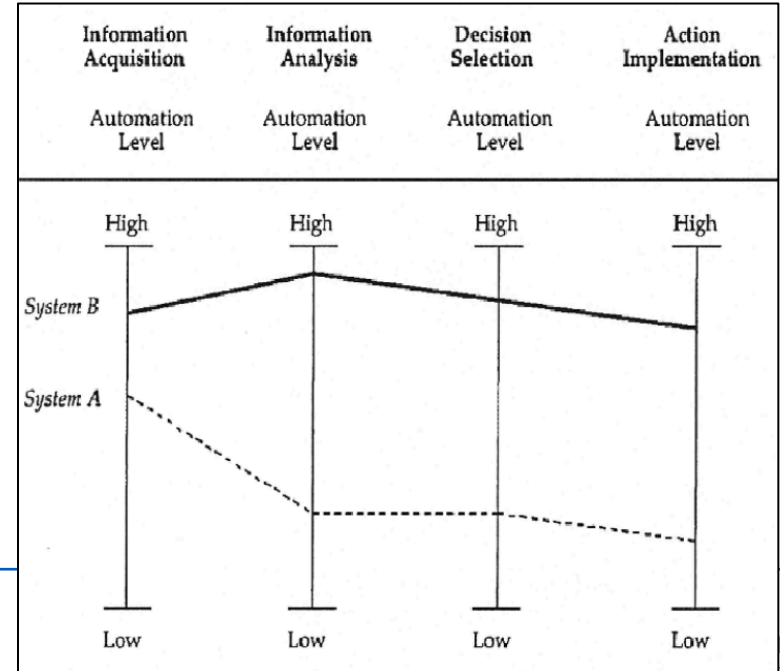


A temporal breakdown of LoA



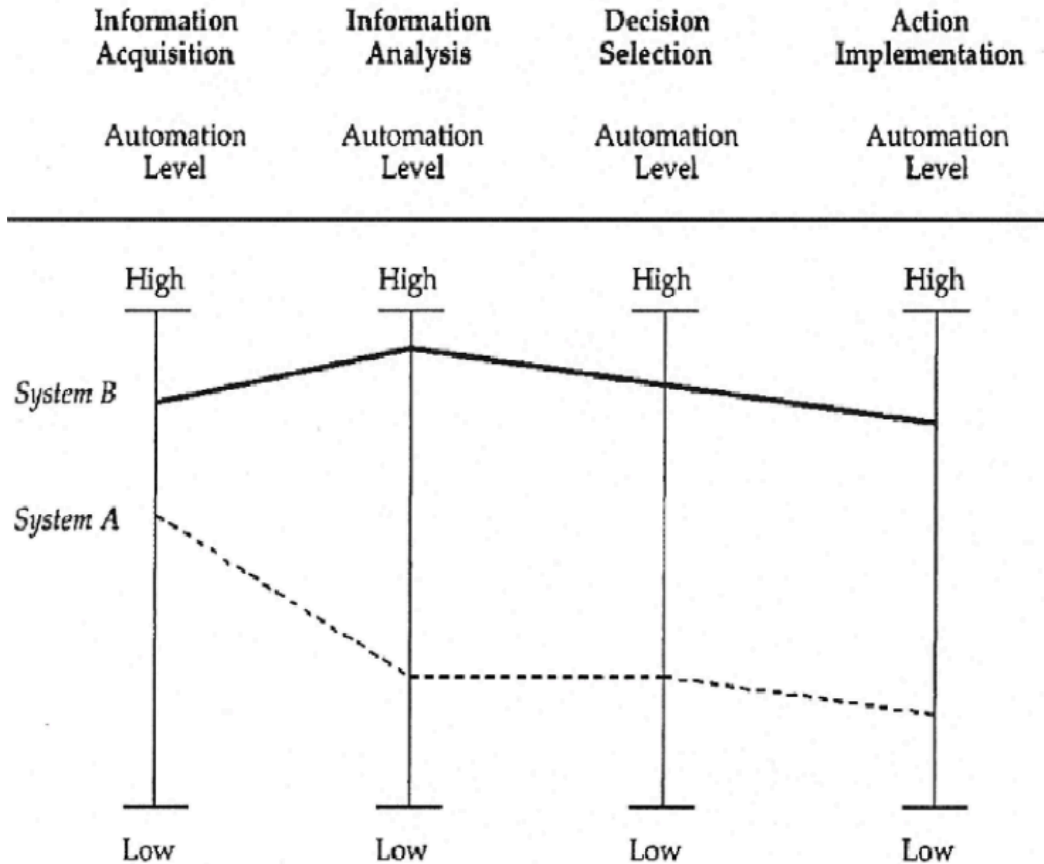


Q: Roomba: Which level at which stage?

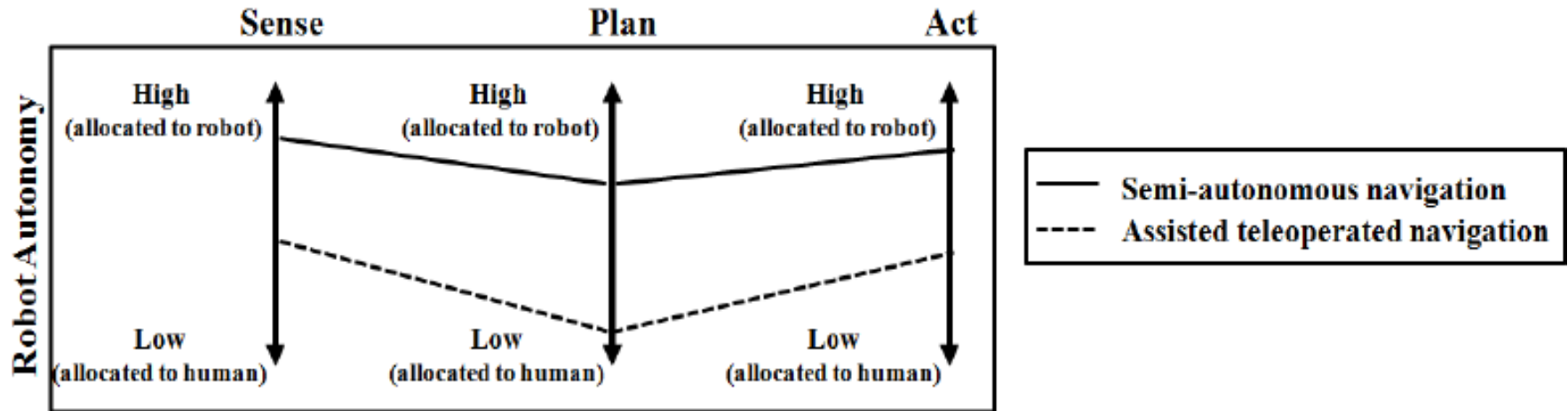




Q: Pick one system you use and draw LoA diagram

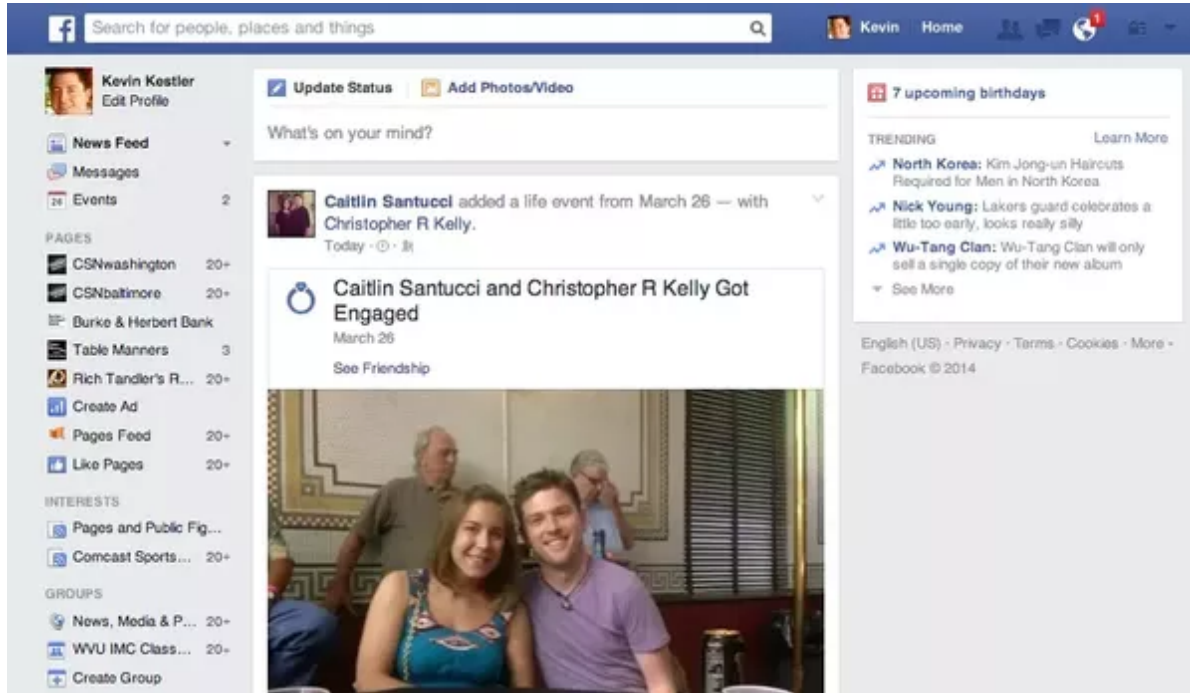


Automation allocation in human-robot interaction





Q: What are the levels of automation used by Facebook?



Reminders

TABLE 2.1: A Scale of Degrees of Automation

1. The computer offers no assistance; the human must do it all.
2. The computer suggests alternative ways to do the task.
3. The computer selects one way to do the task and
4. executes that suggestion if the human approves, or
5. allows the human a restricted time to veto before automatic execution, or
6. executes the suggestion automatically, then necessarily informs the human, or
7. executes the suggestion automatically, then informs the human only if asked.
8. The computer selects the method, executes the task, and ignores the human.



Aalto University

Assignment 4

Assignment 4 overview

A4-1: Task analysis [5p, recommended]

A4-2: Root cause analysis of an accident [5p, optional]