Mental Models

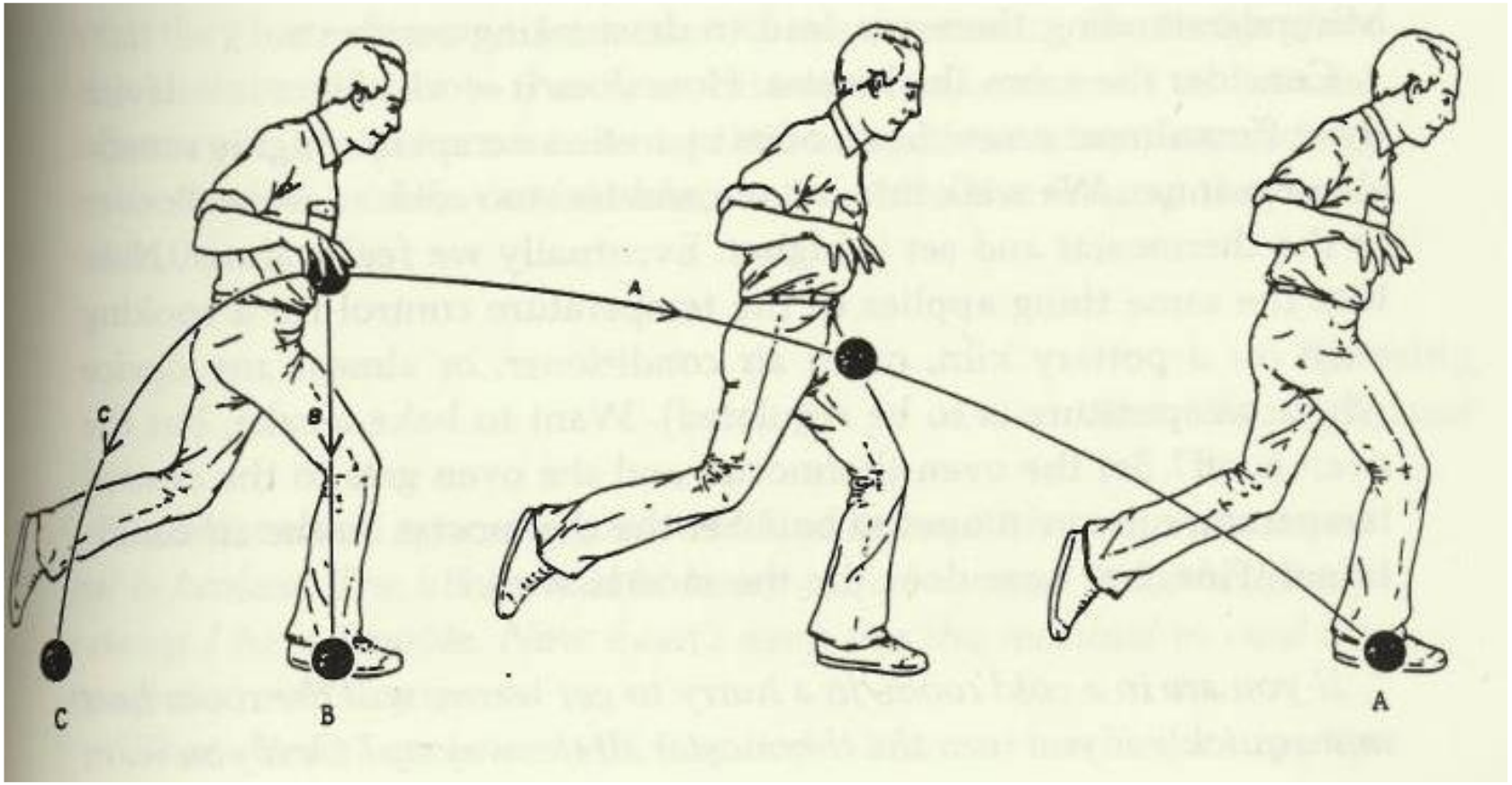
“A mental model is what the user believes about the system at hand.”

-- Jacob Nielsen

Mental Models

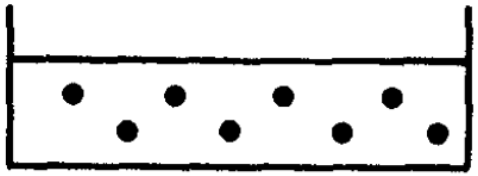
- Representations of systems and environments derived from experiences
- People understand and interact with systems by comparing the outcomes of their mental models with the real-world systems
  - When outcomes match, the model is seen as accurate
  - When outcomes do not match, the model is adjusted
- Two types of mental models
  - System Models – Mental models of how systems work
  - Interaction models – Models of how people interact with systems

If the man drops the ball while running, what path will it take?

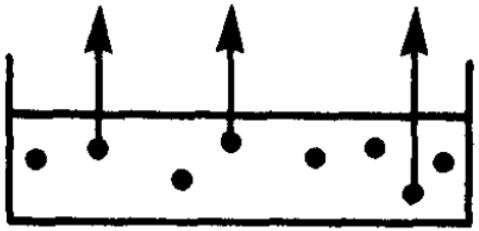


Mental models of water evaporation

Heat Threshold Model

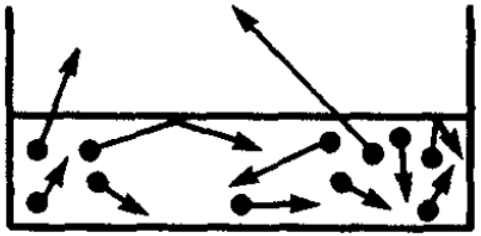


BELOW-BOILING



ABOVE-BOILING

Rocketship Model



Collins, Allan, and Dedre Gentner. "How people construct mental models." *Cultural models in language and thought* (1987)

Mental models of water evaporation

Table 10.4. *Evaporation questions*

Question 1. Which is heavier, a quart container full of water or a quart container full of steam?

Question 2. Why can you see your breath on a cold day?

Question 3. If you put a thin layer of oil on a lake, would you increase, decrease, or cause no change in the rate of evaporation from the lake?

Question 4. Which will evaporate faster, a pan of hot water placed in the refrigerator or the same pan left at room temperature and why?

Question 5. Does evaporation affect water temperature, and if so how? Why or why not?

Question 6. If you wanted to compress some water vapor into a smaller space but keep the pressure constant, what would you do? Why?

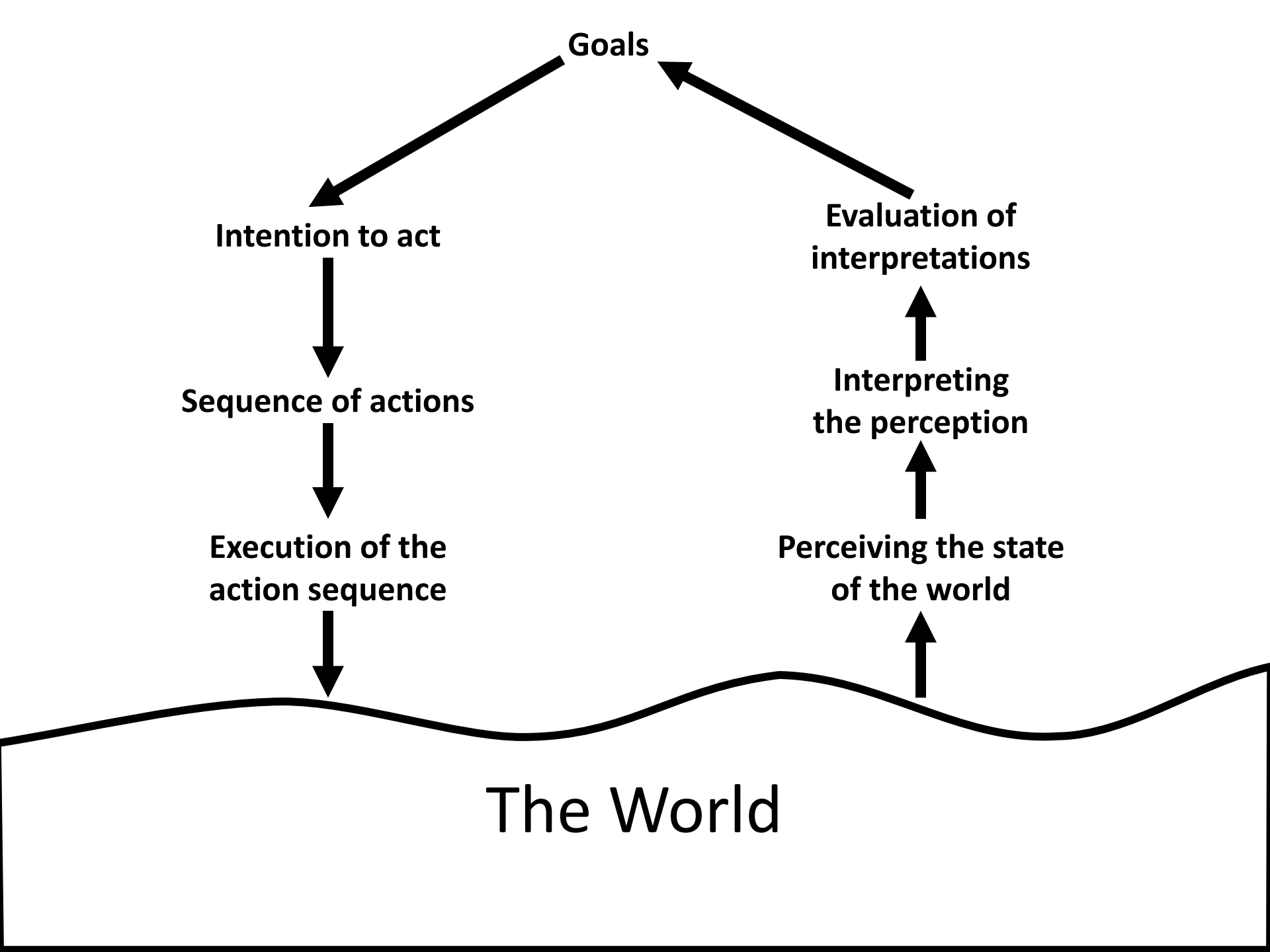
Question 7. On a hot humid day, you must sweat *more* or *less* or *the same amount* as on a hot dry day at the same temperature. Why?

Question 8. If you had two glasses of water sealed in an air-tight container, and one was half filled with pure water, while the other half was filled with salt water, what would you expect to happen after a long period of time (say about a month)? Why?

Collins, Allan, and Dedre Gentner. "How people construct mental models." *Cultural models in language and thought* (1987)

“A user interface is well designed when the program behaves just as the user thought it would.”

-- Joel Spolsky

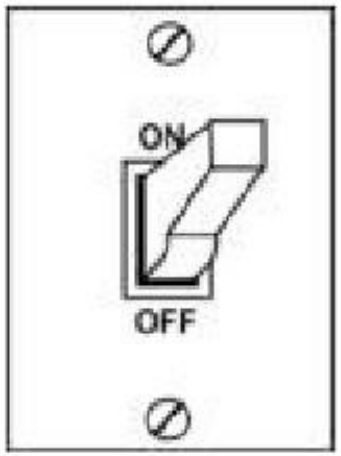

Goals
Intention to act
Sequence of actions
Execution of the action sequence
Evaluation of interpretations
Interpreting the perception
Perceiving the state of the world
The World

The heating has just come on but the room is cold. The room thermostat is set where you normally have it (higher than the current room temperature).

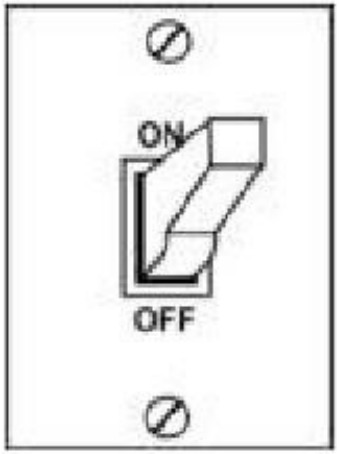
Do you…

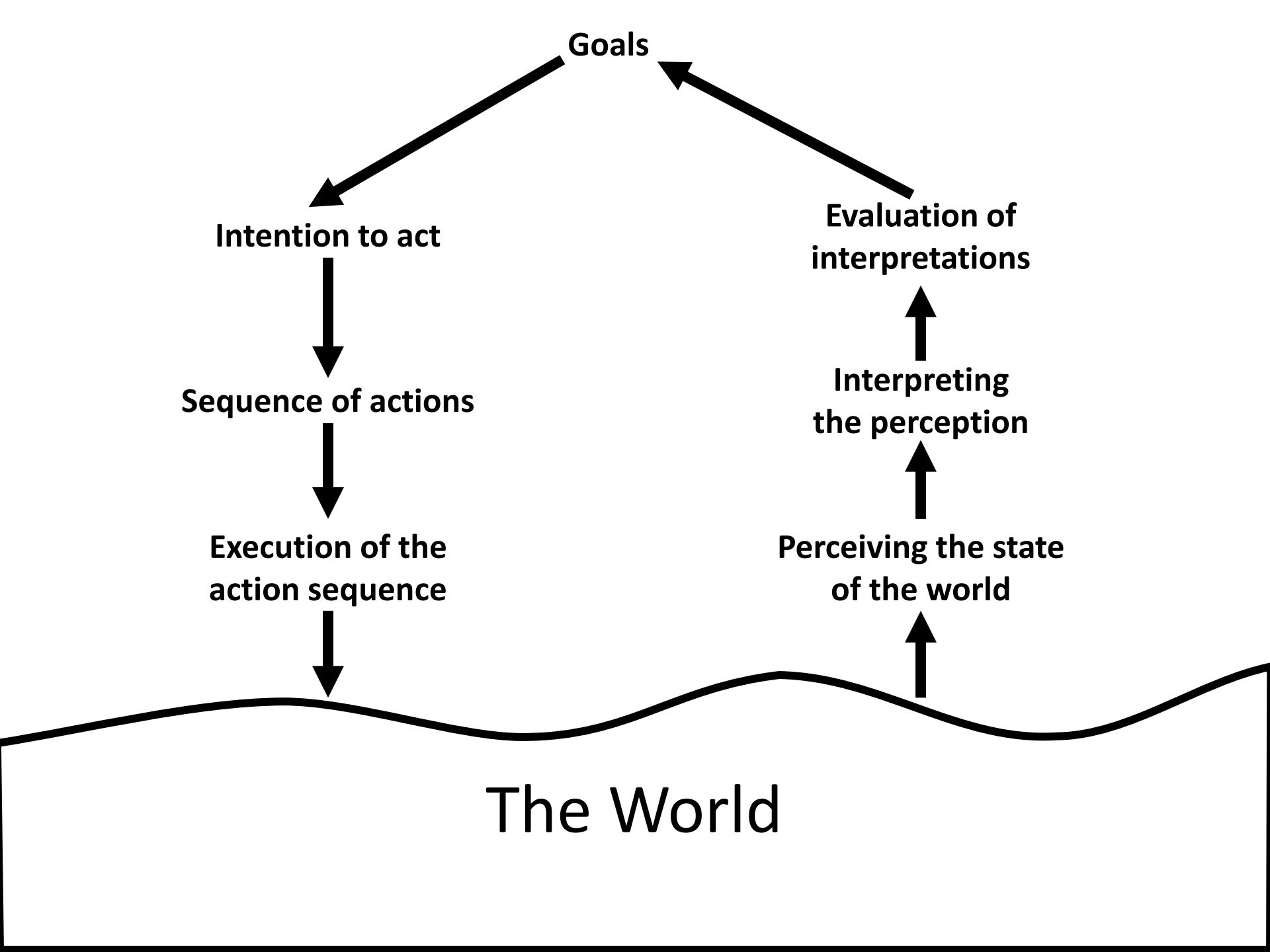
1. Turn it up so the room heats faster
2. Leave it where it is and just wait?

Do room thermostats work like taps or switches?

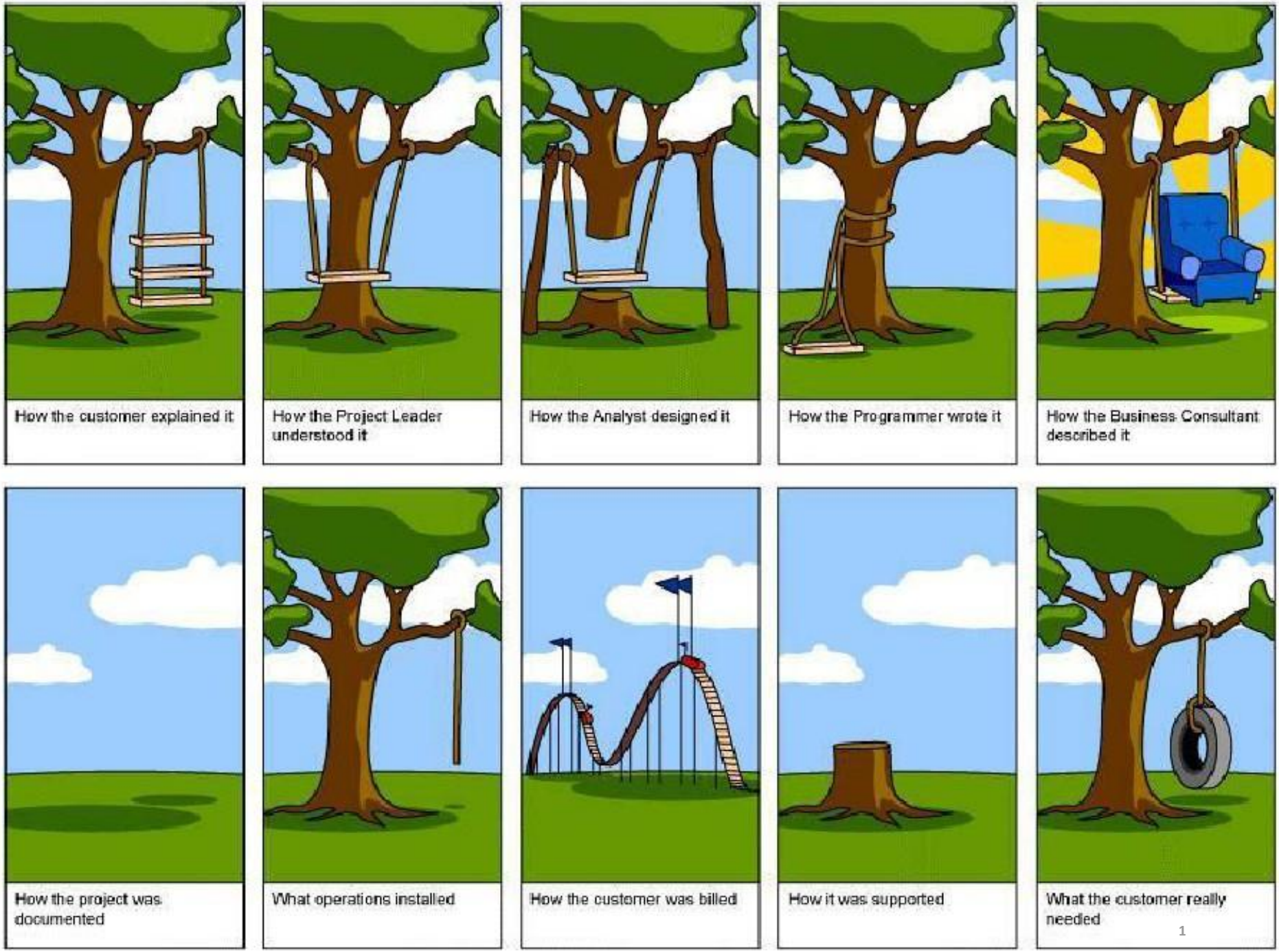


Do room thermostats work like taps or switches?




Goals
Intention to act
Sequence of actions
Execution of the action sequence
Evaluation of interpretations
Interpreting the perception
Perceiving the state of the world
The World

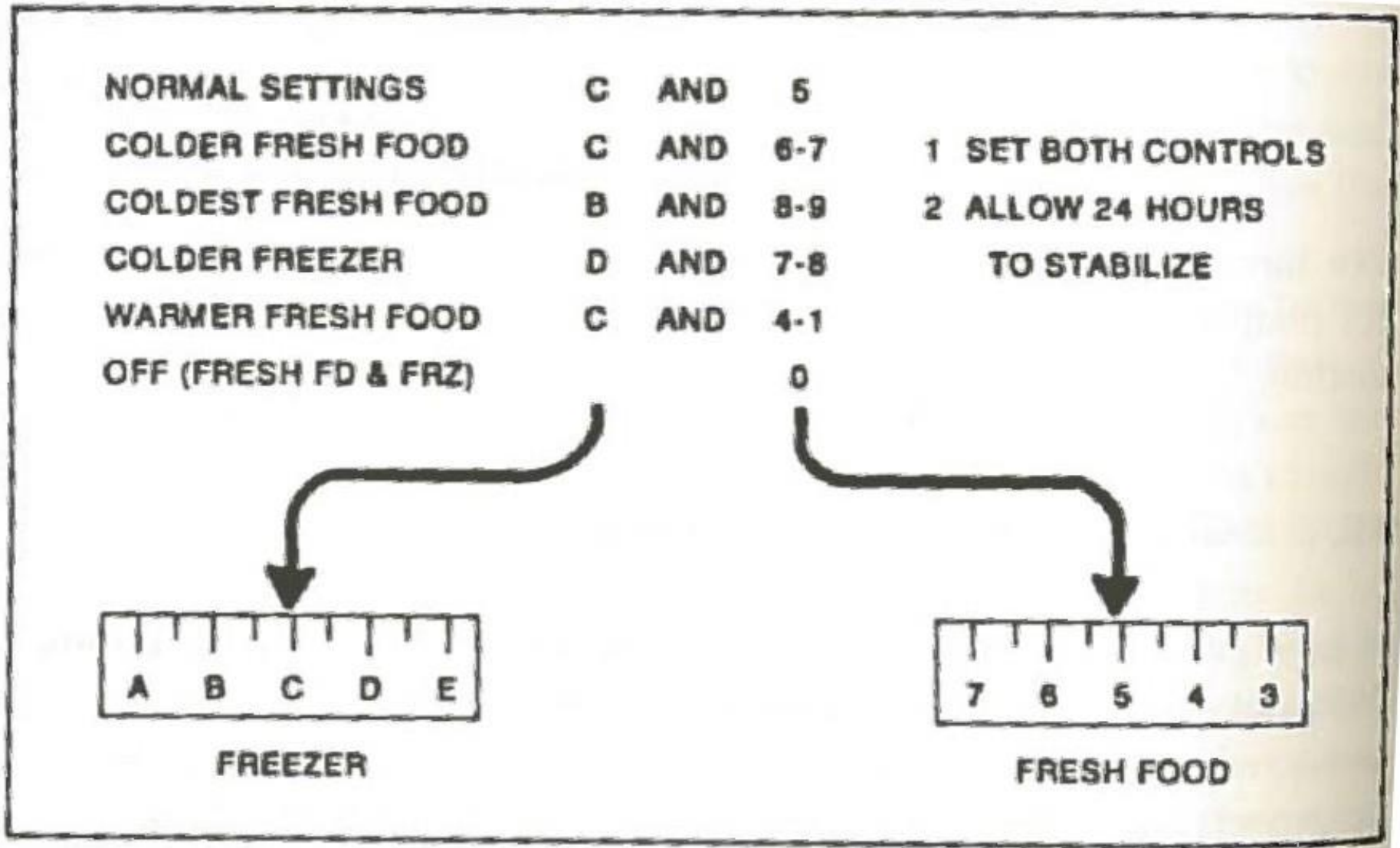
Different people have different mental models of how the system does or should work.


How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
How the project was documented
What operations installed
How the customer was billed
How it was supported
What the customer really needed

There are three models of the system

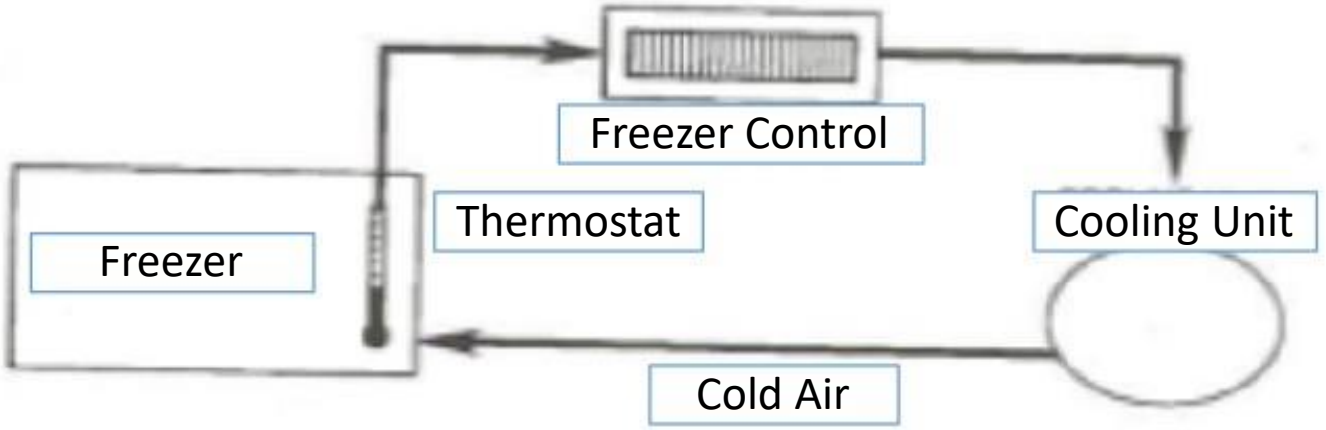
- User Model - How the user thinks the product works. The mental model.
- UI Model - How the product is presented to the user in the user interface.
- Implementation Model - How the product is actually implemented.

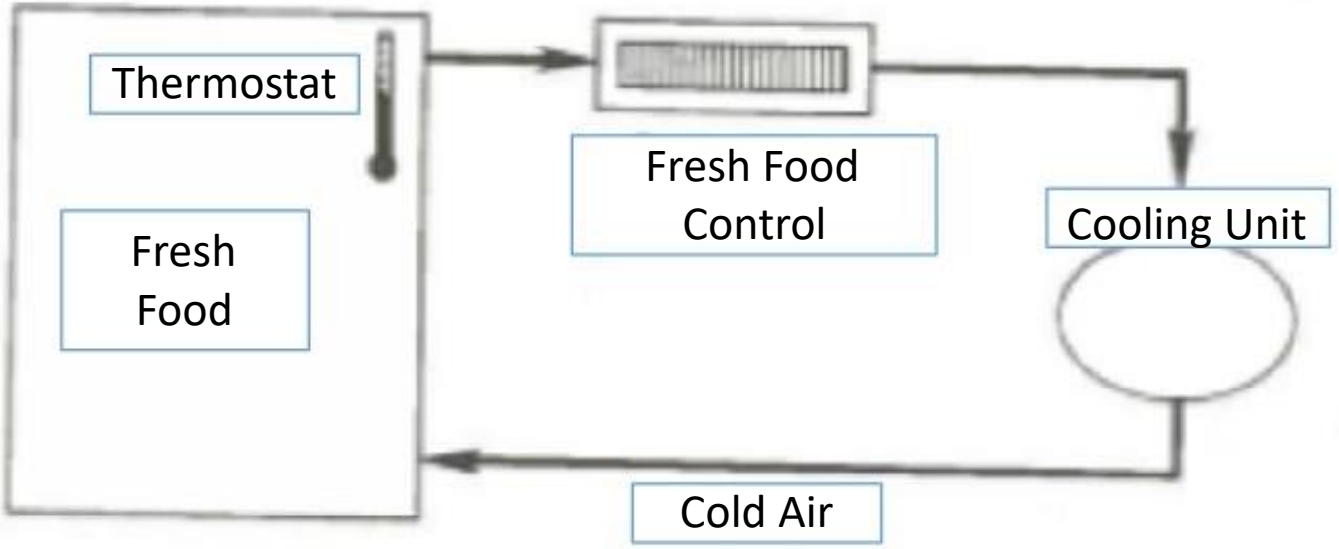
UI Model (refrigerator temperature)



The design of Everyday Things by Donald Norman

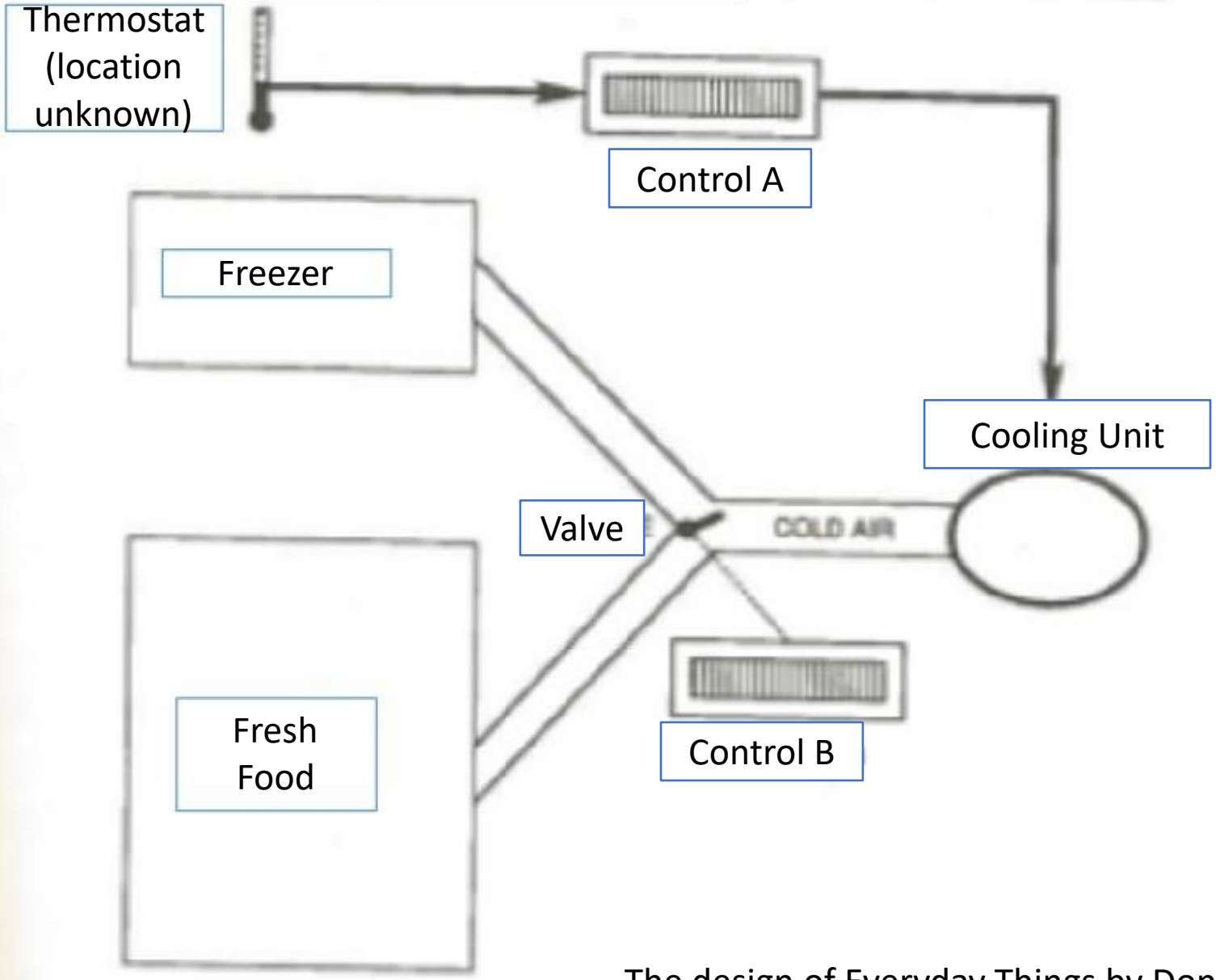
User mental model





The design of Everyday Things by Donald Norman

Implemented model



The design of Everyday Things by Donald Norman

Good user interfaces help the user develop a good mental model of the system.

One way to help the user build a mental model is through explanation and analogy (a is like b).

What is a Virus? (Folk Models)

- Viruses are bad software
  - Viruses are bad, but not much more is known about them
- Viruses are buggy software
  - Viruses are just mistakes in software that can cause you trouble
- Viruses cause mischief
  - Viruses are there to intentionally annoy users
- Viruses support crime
  - Viruses steal information like credit card data

VIRUS ALERT!

Is your antivirus on watch?

An antivirus is software that prevents, detects, and removes malicious software like computer viruses, worms, trojan horses, spyware, adware, and other types of malware.

Virus Detection Methods

SIGNATURE BASED DETECTION

An antivirus works with a database of known viruses. Each virus is identified by its uniquely recognized coded sequences, called the virus fingerprint.

The database needs to be updated often so it knows what viruses to look for!

The term "virus" commonly refers to many different kinds of malware.

SUSPICIOUS BEHAVIOUR BASED DETECTION

An antivirus can also recognize new viruses based on heuristics derived from virus behaviours previously seen.

This method can be effective for detecting new viruses that are not yet stored in the database.

PREMISE PROTECTED
ANTIVIRUS ON WATCH

Tips to Stay Vigilant

When in doubt, always err on the side of caution. Be cautious when opening, downloading, or executing any files or email attachments.

Maintain an updated antivirus.
To protect yourself from getting infected, keep your antivirus software up-to-date.

Myth: Multiple antivirus programs are beneficial.
Fact: Having ONE updated antivirus software is better than installing multiple incompatible programs.

Myth: Having an antivirus is enough.
Fact: Take a multi-layered approach to computer security that includes protection such as an antivirus program, and being cautious online.

Practice safe internet habits.
Download files from reliable sources, and avoid insecure file-sharing programs.

Myth: I don't use the internet so I can't get a virus.
Fact: Even if you don't use the internet, inserting infected external drives like USBs can transfer viruses onto your computer.

Myth: I don't visit "shady" sites so I can't get a virus.
Fact: You could still get infected through legitimate websites that have been compromised, and through phishing sites, which are malicious clones of popular or trusted websites.

Install the latest system security updates.
Reduce the vulnerability of your OS by keeping it updated to the latest version.

Myth: Macs are far more secure than PCs.
Fact: The market share of Windows is higher than Apple's OS, making PCs bigger targets. As Macs become more popular, they are also becoming attractive targets for hackers.

Myth: Viruses damage your computer's hardware.
Fact: Viruses cannot physically damage hardware, but might indirectly affect how hardware behaves.

VIRUS ALERT!

Is your antivirus on watch?

An antivirus is software that prevents, detects, and removes malicious software like computer viruses, worms, trojan horses, spyware, adware, and other types of malware.

Tips to Stay Vigilant

When in doubt, always err on the side of caution. Be cautious when opening, downloading, or executing any files or email attachments.

Maintain an updated antivirus.
To protect yourself from getting infected, keep your antivirus software up-to-date.

Myth: **Multiple antivirus programs are beneficial.**
Fact: Having ONE updated antivirus software is better than installing multiple incompatible programs.

Myth: **Having an antivirus is enough.**
Fact: Take a multi-layered approach to computer security that includes protection such as an antivirus program, and being cautious online.

Virus Detection Methods

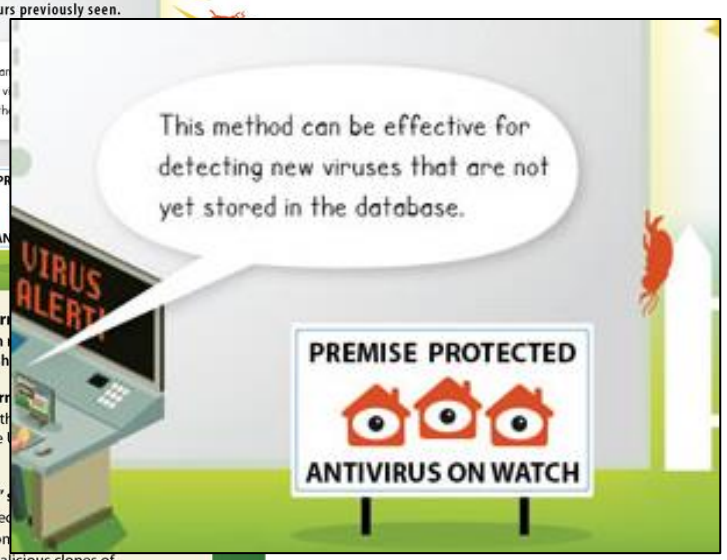
SIGNATURE BASED DETECTION

antivirus works with a database of own viruses. Each virus is identified its uniquely recognized coded quences, called the virus fingerprint.

The term "virus" commonly refers to many different kinds of malware.

SUSPICIOUS BEHAVIOUR BASED DETECTION

An antivirus can also recognize new viruses based on heuristics derived from virus behaviours previously seen.



Tips to Stay Vigilant

always err on the side of caution.
en opening, downloading, or
iles or email attachments.

Practice safe inter
Download files from
avoid insecure file-sh

Myth: **I don't use the interr**
Fact: Even if you don't use t
infected external drives like
onto your computer.

Myth: **I don't visit "shady"**
Fact: You could still get infe
websites that have been co
phishing sites, which are malicious clones of popular or trusted websites.

Maintain an updated antivirus.
To protect yourself from getting infected, keep your antivirus software up-to-date.

Myth: **Multiple antivirus programs are beneficial.**
Fact: Having ONE updated antivirus software is better than installing multiple incompatible programs.

Myth: **Having an antivirus is enough.**
Fact: Take a multi-layered approach to computer security that includes protection such as an antivirus program, and being cautious online.

Install the latest system security updates.
Reduce the vulnerability of your OS by keeping it updated to the latest version.

Myth: **Macs are far more secure than PCs.**
Fact: The market share of Windows is higher than Apple's OS, making PCs bigger targets. As Macs become more popular, they are also becoming attractive targets for hackers.

Myth: **Viruses damage your computer's hardware.**
Fact: Viruses cannot physically damage hardware, but might indirectly affect how hardware behaves.

ANTIVIRUS SOFTWARE

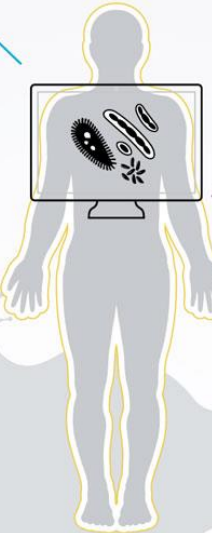
Boosting Computers' Immune System

An **antivirus** is software that prevents, detects, and removes malicious software like computer viruses, worms, trojan horses, spyware, adware, and other types of malware.

VIRUS DETECTION METHODS

SIGNATURE BASED DETECTION

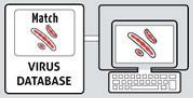
An antivirus works with a database of known viruses. Each virus is identified by its uniquely recognized coded sequences, called the virus fingerprint.



The term **"virus"** commonly refers to many different kinds of **malware**.

SUSPICIOUS BEHAVIOUR BASED DETECTION

An antivirus can sometimes recognize new viruses based on heuristics derived from virus behaviours previously seen.



The virus database needs to be updated often so it knows what viruses to look for!

Suspicious behaviour based detection can be effective for detecting new viruses that are not yet stored in the database.

TIPS TO STAY HEALTHY

Maintain an updated antivirus

To protect yourself from getting infected, keep your antivirus software up-to-date.

Myth: Multiple antivirus programs are beneficial.
Fact: Having ONE updated antivirus software is better than installing multiple incompatible programs.

Myth: Having an antivirus is enough.
Fact: Take a multi-layered approach to computer security that includes protection such as an antivirus program, and being cautious online.

Install the latest system security updates

Reduce the vulnerability of your OS by keeping it updated to the latest version.

Myth: Macs are far more secure than PCs.
Fact: The market share of Windows is higher than Apple's OS, making PCs bigger targets. As Macs become more popular, they are also becoming attractive targets for hackers.

Myth: Viruses damage your computer's hardware.
Fact: Viruses cannot physically damage hardware, but might indirectly affect how hardware behaves.

Practice safe internet habits

Download files from reliable sources, and avoid insecure file-sharing programs.

Myth: I don't use the internet so I can't get a virus.
Fact: Even if you don't use the internet, inserting infected external drives like USBs can transfer viruses onto your computer.

Myth: I don't visit "shady" sites so I can't get a virus.
Fact: You could still get infected through legitimate websites that have been compromised, and through phishing sites, which are malicious clones of popular or trusted websites.

ANTIVIRUS SOFTWARE

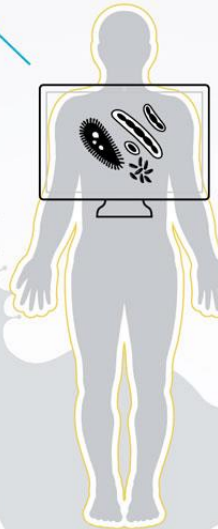
Boosting Computers' Immune System

An **antivirus** is software that prevents, detects, and removes malicious software like computer viruses, worms, trojan horses, spyware, adware, and other types of malware.

VIRUS DETECTION METHODS

SIGNATURE BASED DETECTION

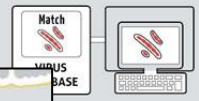
An antivirus works with a database of known viruses. Each virus is identified by its uniquely recognized coded sequences, called the virus fingerprint.



The term "virus" commonly refers to many different kinds of malware.

SUSPICIOUS BEHAVIOUR BASED DETECTION

An antivirus can sometimes recognize new viruses based on heuristics derived from virus behaviours previously seen.



s database needs to
ted often so it knows
uses to look for!

Suspicious behaviour based
detection can be effective fo
detecting new viruses that a
not yet stored in the database

TIPS TO STAY HEALTHY

Maintain an updated antivirus
To protect yourself from getting infected, keep your antivirus software up-to-date.

Myth: Multiple antivirus programs are beneficial.
Fact: Having ONE updated antivirus software is better than installing multiple incompatible programs.

Myth: Having an antivirus is enough.
Fact: Take a multi-layered approach to computer security that includes protection such as an antivirus program, and being cautious online.

TIPS TO STAY HEALTHY

ntain an updated antivirus
rotect yourself from getting infected,
your antivirus software up-to-date.

iple antivirus programs are beneficial.
g ONE updated antivirus software is better
ing multiple incompatible programs.

Myth: Having an antivirus is enough.
Fact: Take a multi-layered approach to computer security that includes protection such as an antivirus program, and being cautious online.

Install the latest system security u
Reduce the vulnerability of your OS b
keeping it updated to the latest versi

Myth: Macs are far more secure than PCs
Fact: The market share of Windows is highe
Apple's OS, making PCs bigger targets. As
become more popular, they are also becom
attractive targets for hackers.

Myth: Viruses damage your computer's h
Fact: Viruses cannot physically damage har
but might indirectly affect how hardware be

Practice safe internet habits
Download files from reliable sources, and avoid insecure file-sharing programs.

Myth: I don't use the internet so I can't get a virus.
Fact: Even if you don't use the internet, inserting infected external drives like USBs can transfer viruses onto your computer.

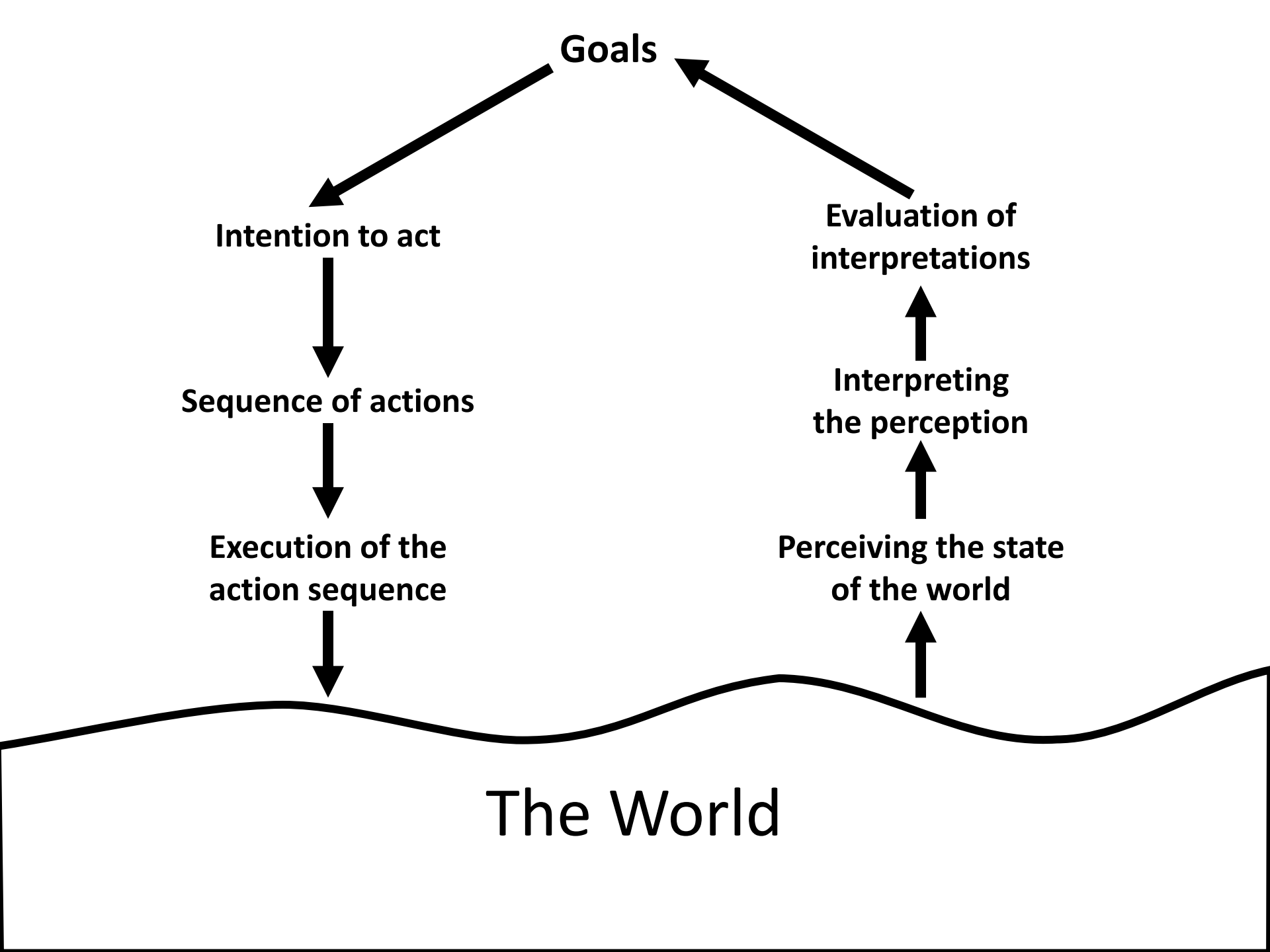
Myth: I don't visit "shady" sites so I can't get a virus.
Fact: You could still get infected through legitimate websites that have been compromised, and through phishing sites, which are malicious clones of popular or trusted websites.

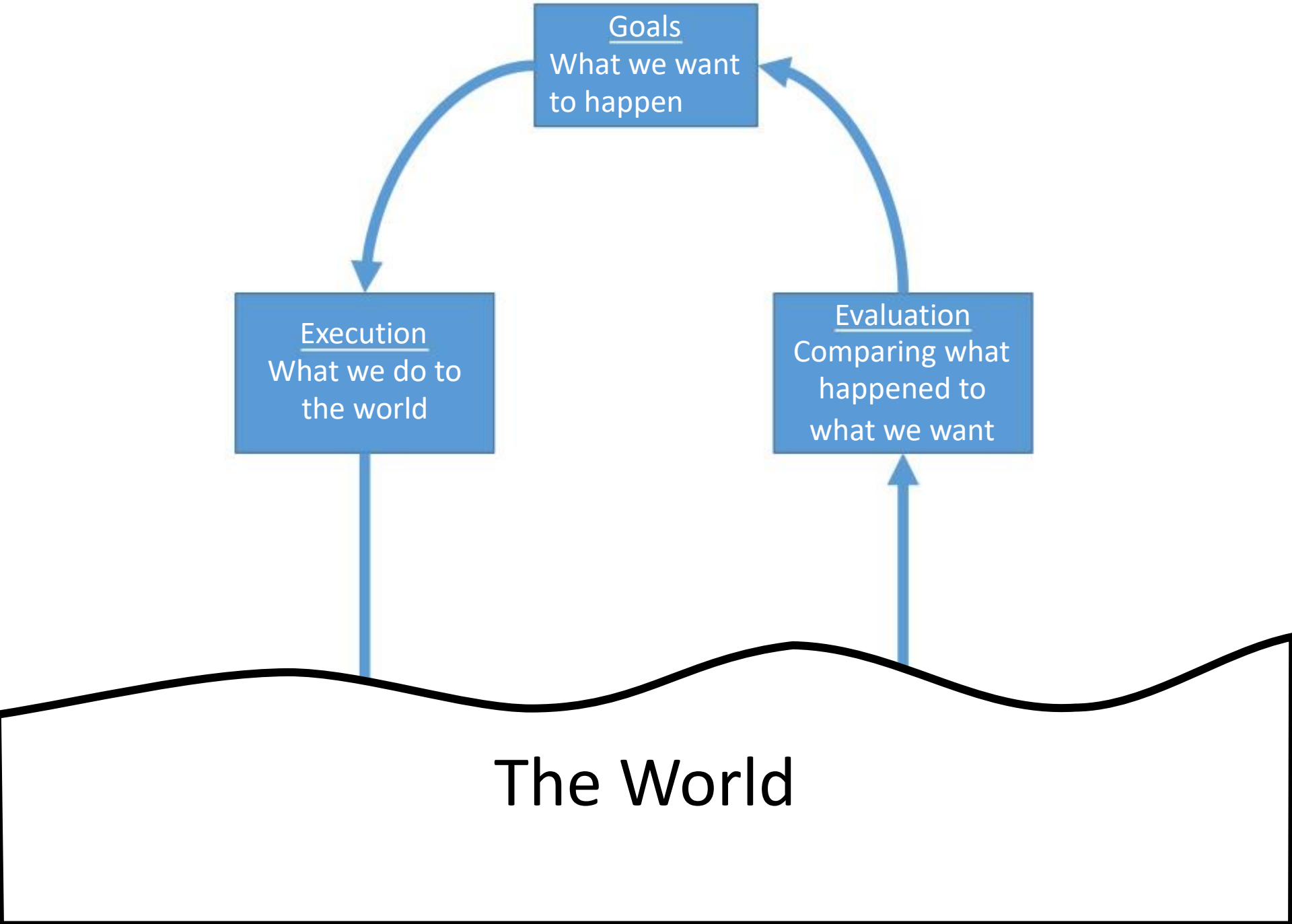
When in doubt, always err on the side of caution. Be cautious when opening, downloading, or executing any files or email attachments.

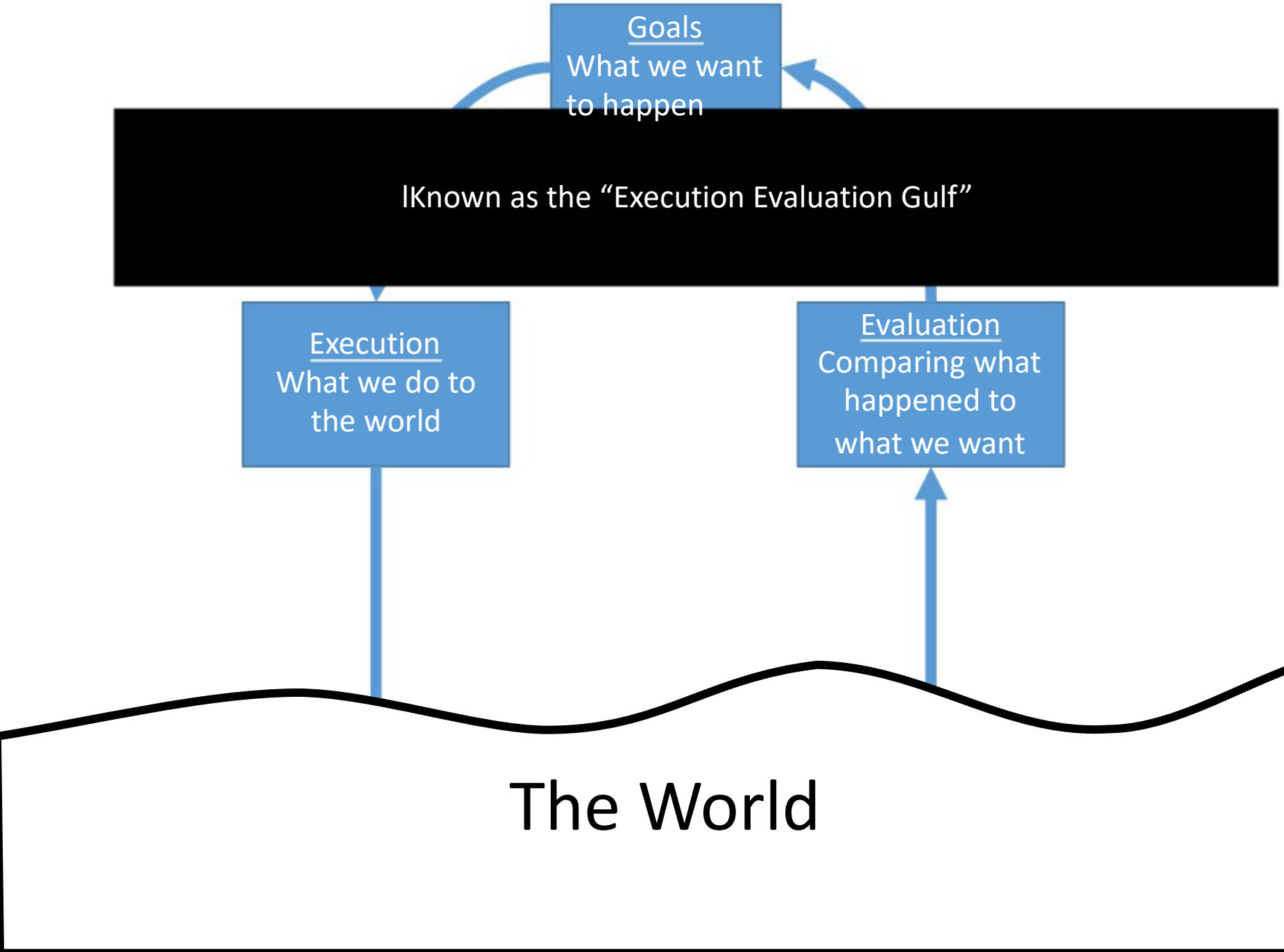
SUSPICIOUS BEHAVIOUR BASED DETECTION

An antivirus can sometimes recognize new viruses based on heuristics derived from virus behaviours previously seen.

Suspicious behaviour based detection can be effective for detecting new viruses that are not yet stored in the database.


Goals
Intention to act
Sequence of actions
Execution of the action sequence
Evaluation of interpretations
Interpreting the perception
Perceiving the state of the world
The World


Goals
What we want to happen
Execution
What we do to the world
Evaluation
Comparing what happened to what we want
The World


Goals
What we want to happen
lKnown as the “Execution Evaluation Gulf”
Execution
What we do to the world
Evaluation
Comparing what happened to what we want
The World

Good user interfaces help the user develop a good mental model of the system

Another way is to support the construction of a mental model.

Package tracking application on first use should support mental model development