goto;

GOTO
CHICAGO 2023

#GOTOchgo

goto;

How to reverse software entropy

Saleem Siddiqui

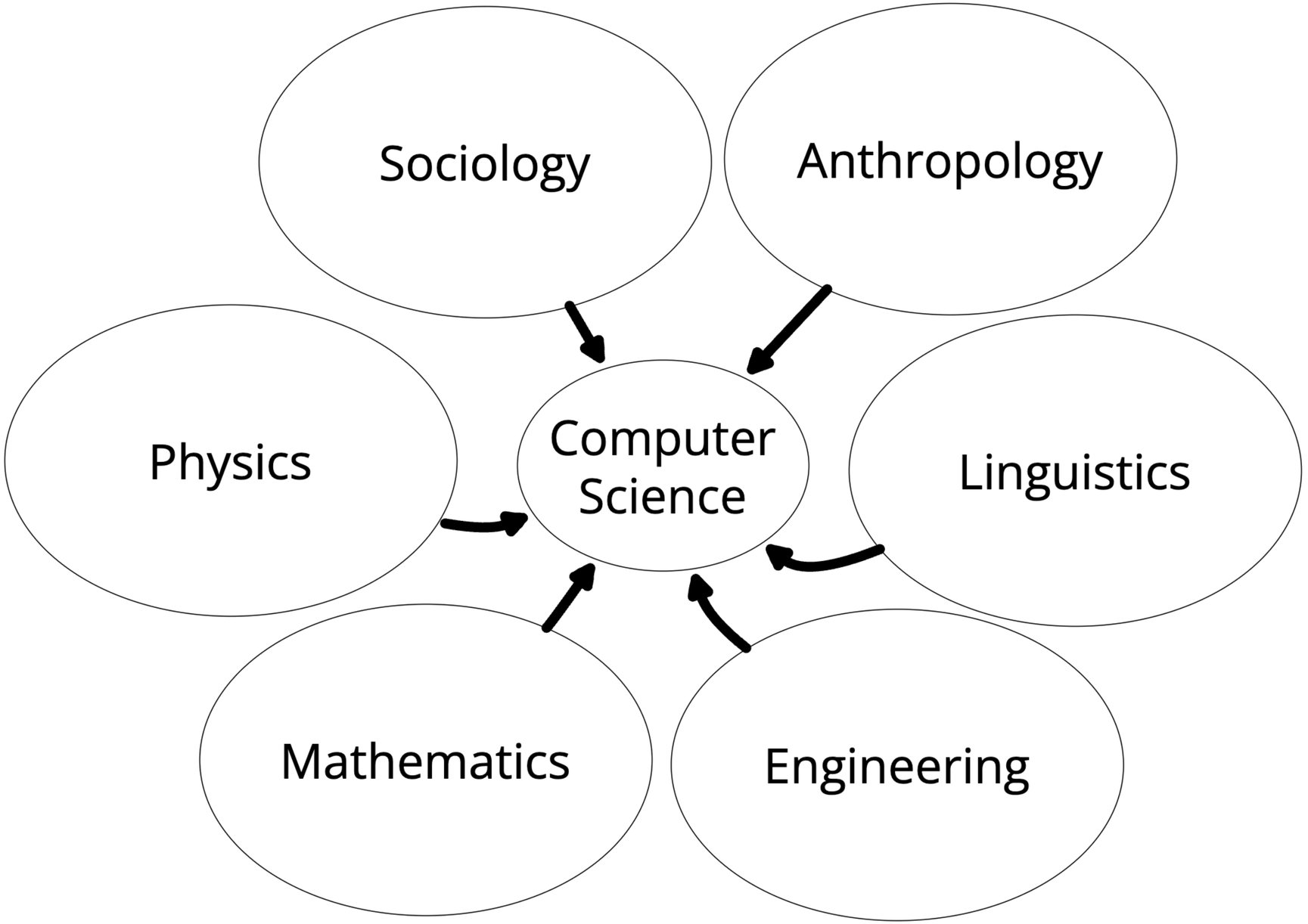
goto;

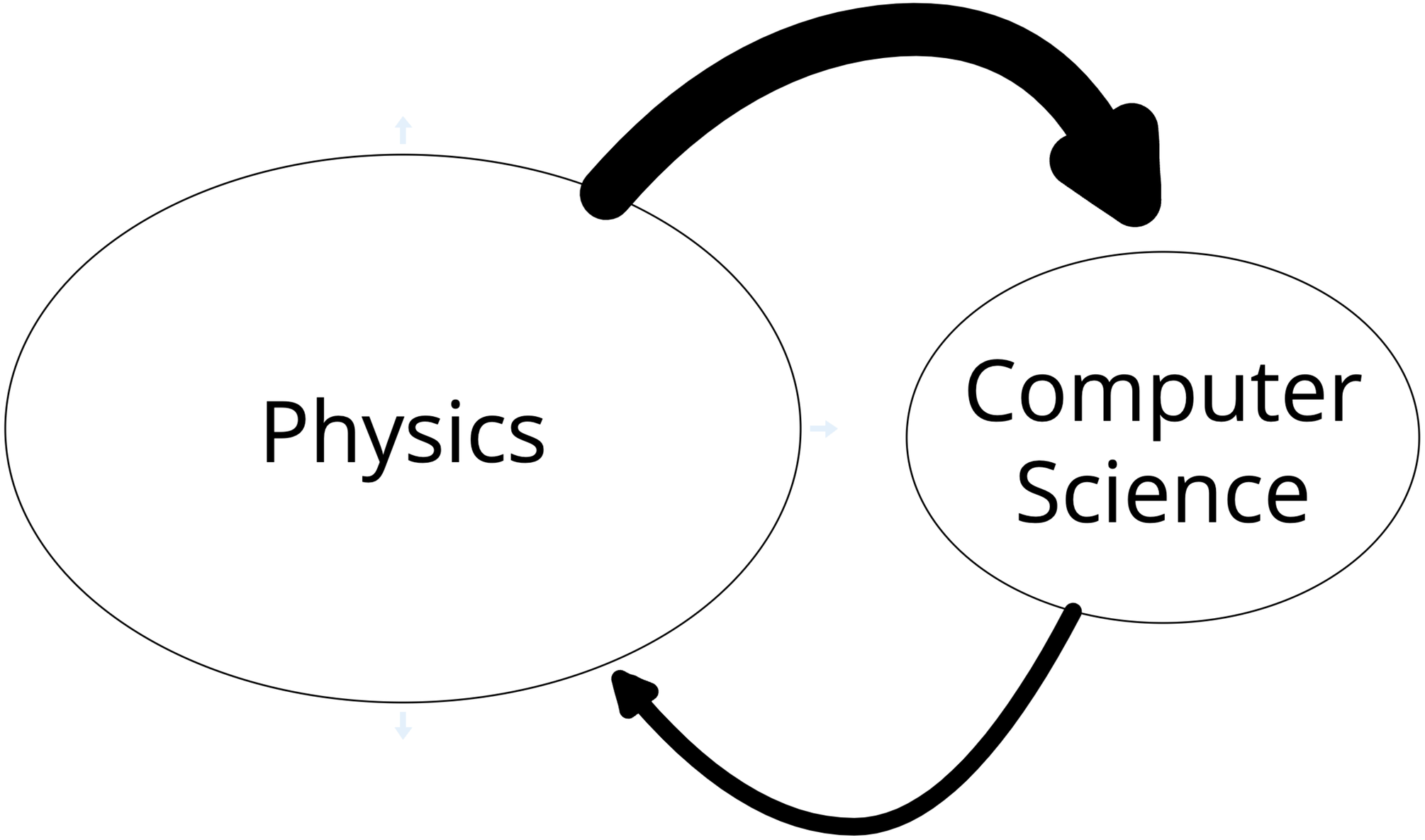
goto;

GOTO CHICAGO 2023

May 22-24, 2023

Technologist, Author, Speaker

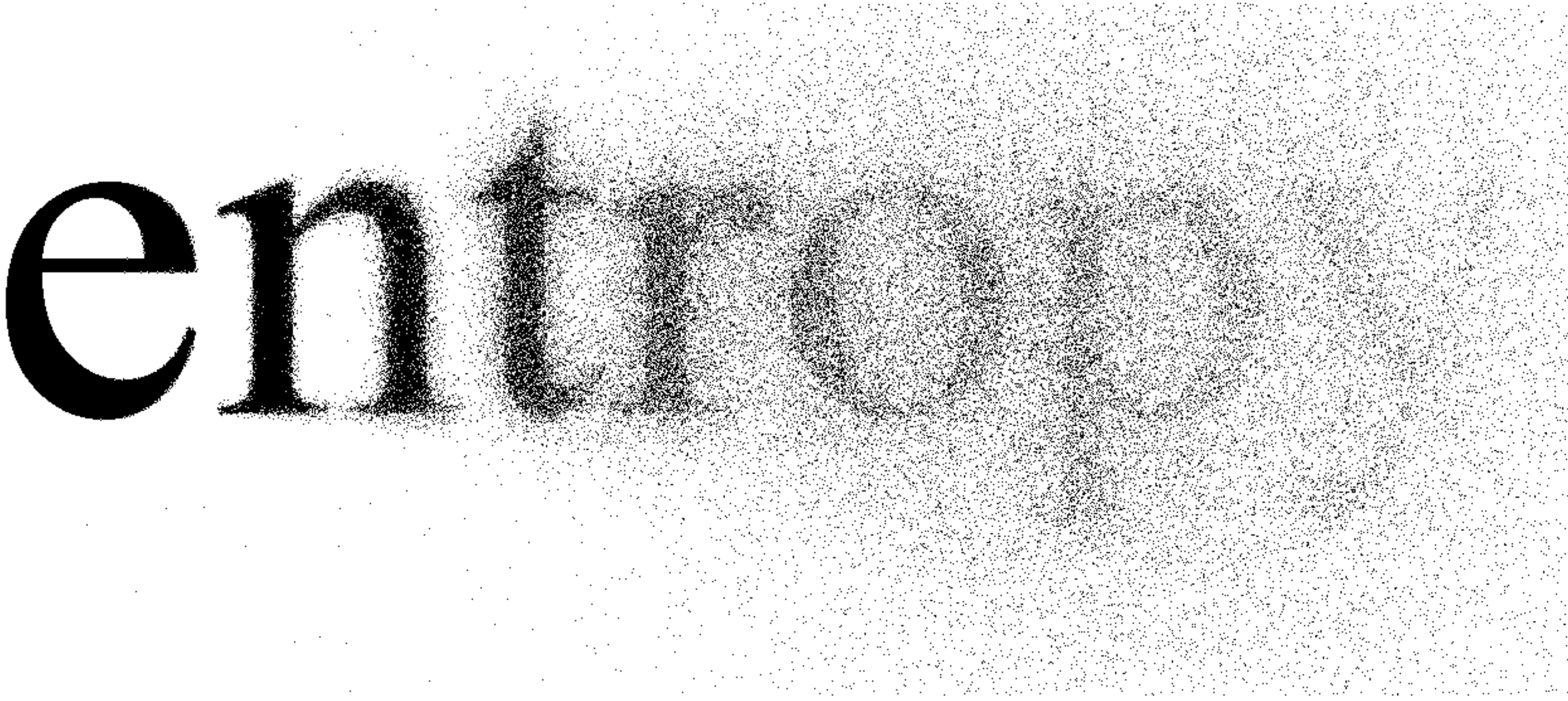

Sociology
Anthropology
Physics
Computer Science
Linguistics
Mathematics
Engineering

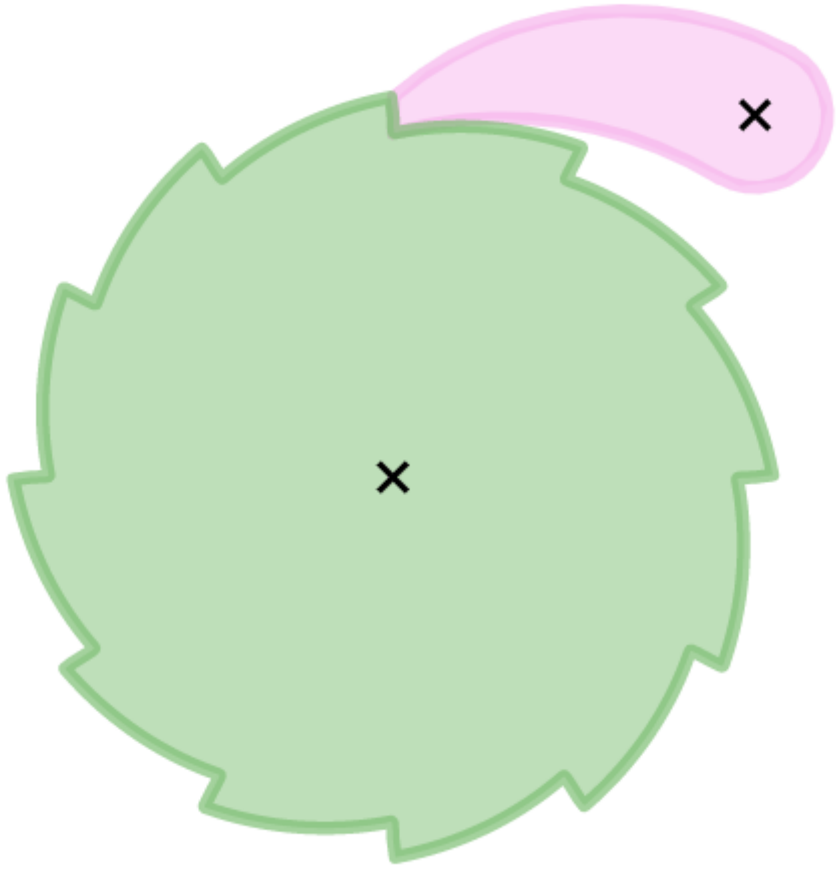

Physics
Computer Science

Computer science is not as old as physics; it lags by a couple of hundred years. However, this does not mean that there is significantly less on the computer scientist's plate than on the physicist's: younger it may be, but it has had a far more intense upbringing!

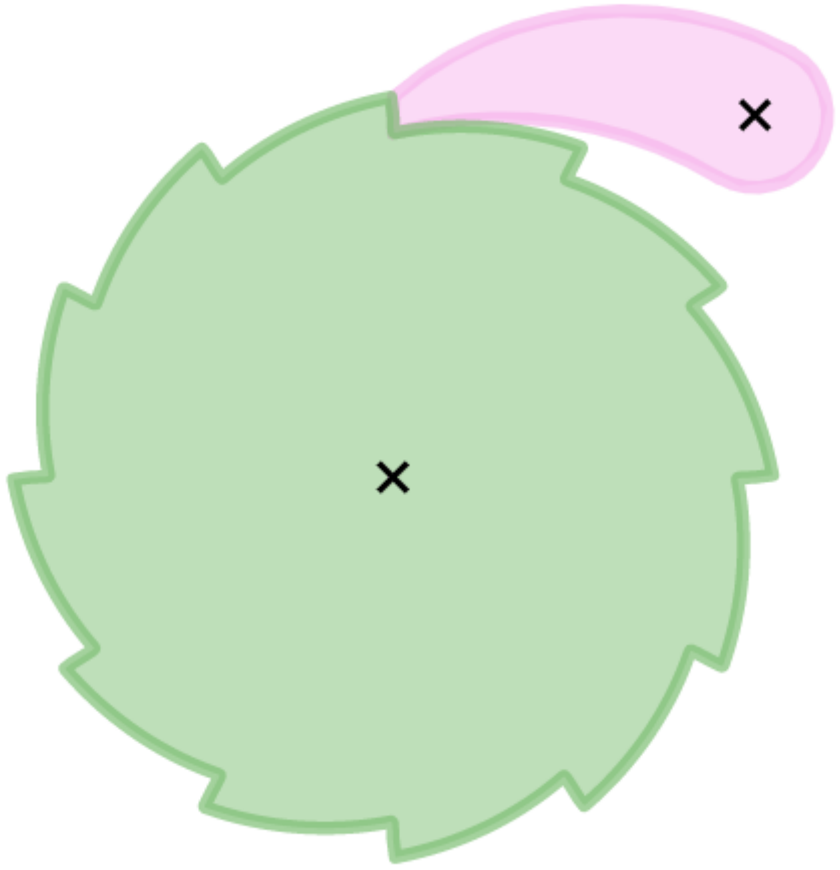
— Richard P. Feynman —

AZ QUOTES


end



The entropy of
an isolated system
must always increase
until it reaches equilibrium –
at maximum entropy.



The entropy of
an isolated **software** system
must always increase
until it reaches equilibrium –
at maximum entropy.

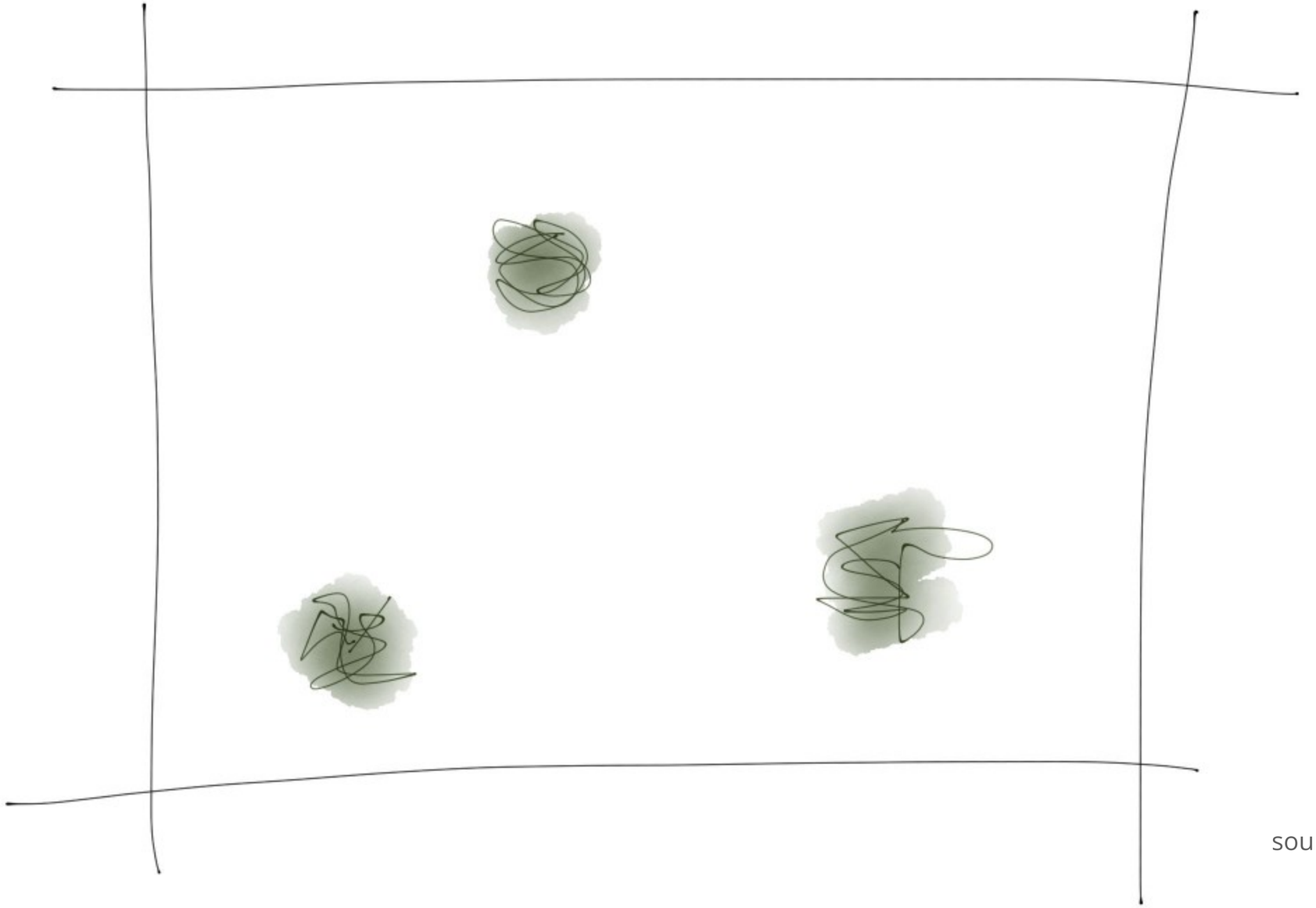
Defining Software Entropy

Defining Software Entropy

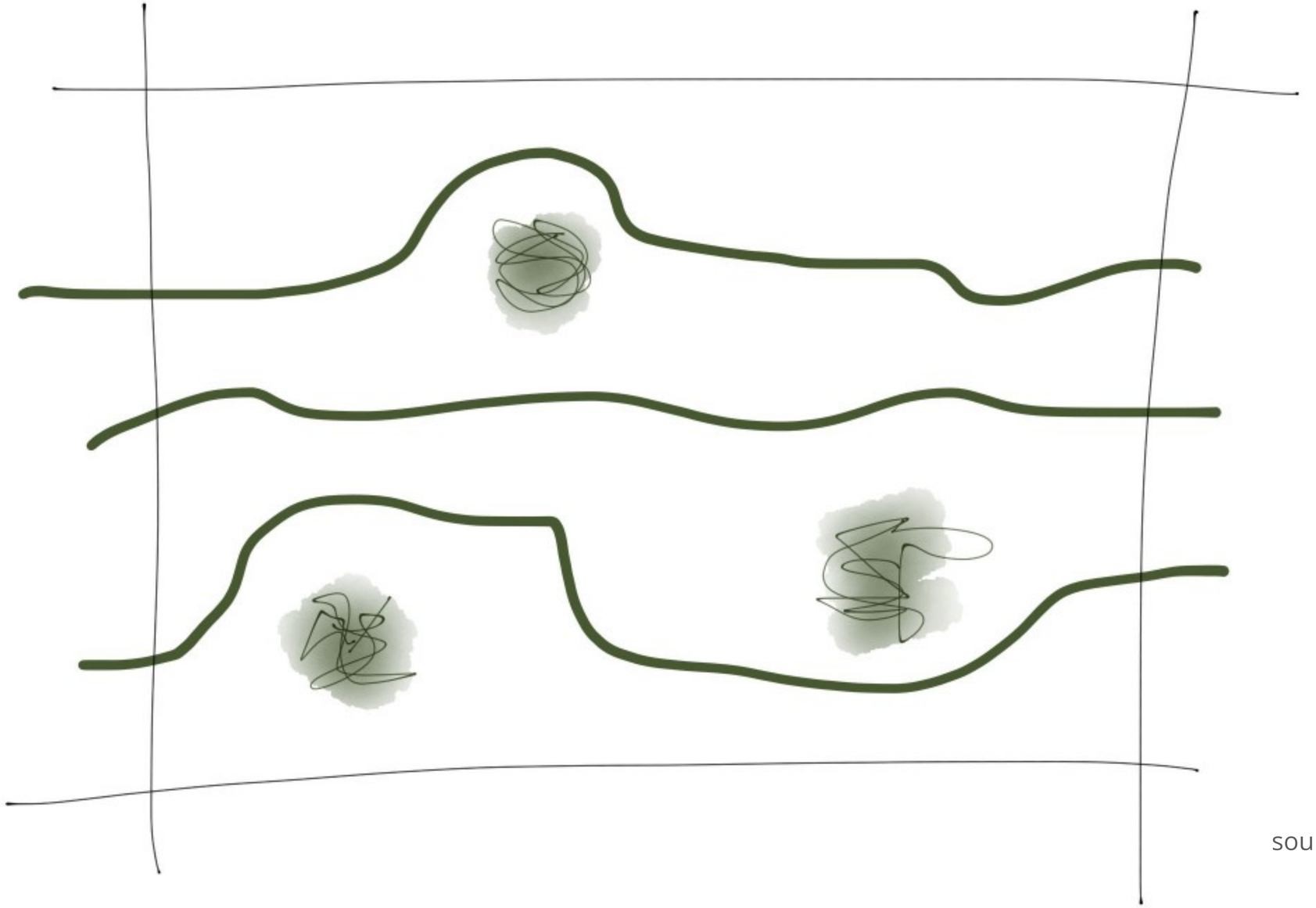
goto;

- The number of files changed with each commit in the source control system.
  – *Kamiel Wanrooij*

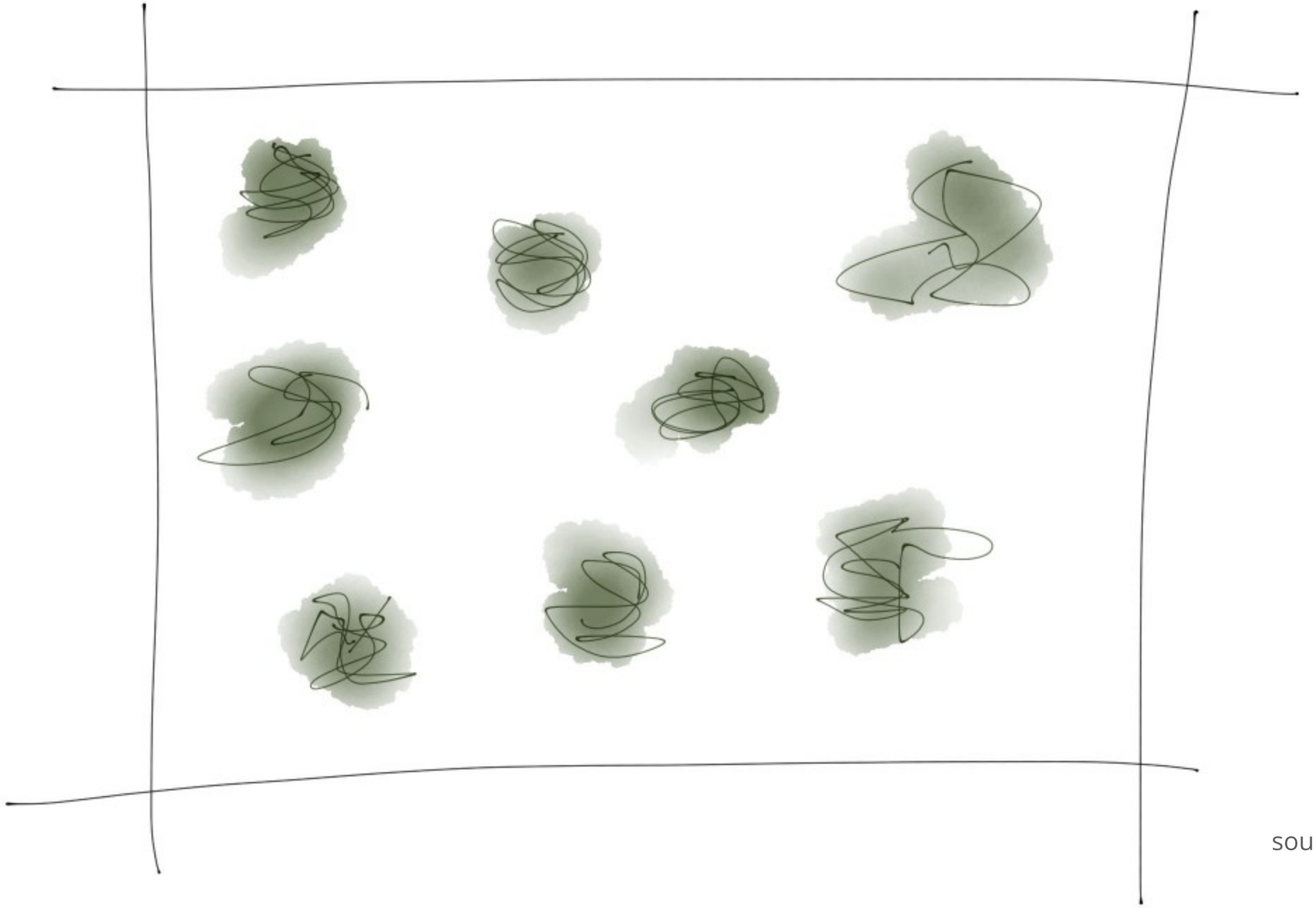
- The ratio of unexpected problems to the scope of work in an iteration.
  – *Adam Wasserman*



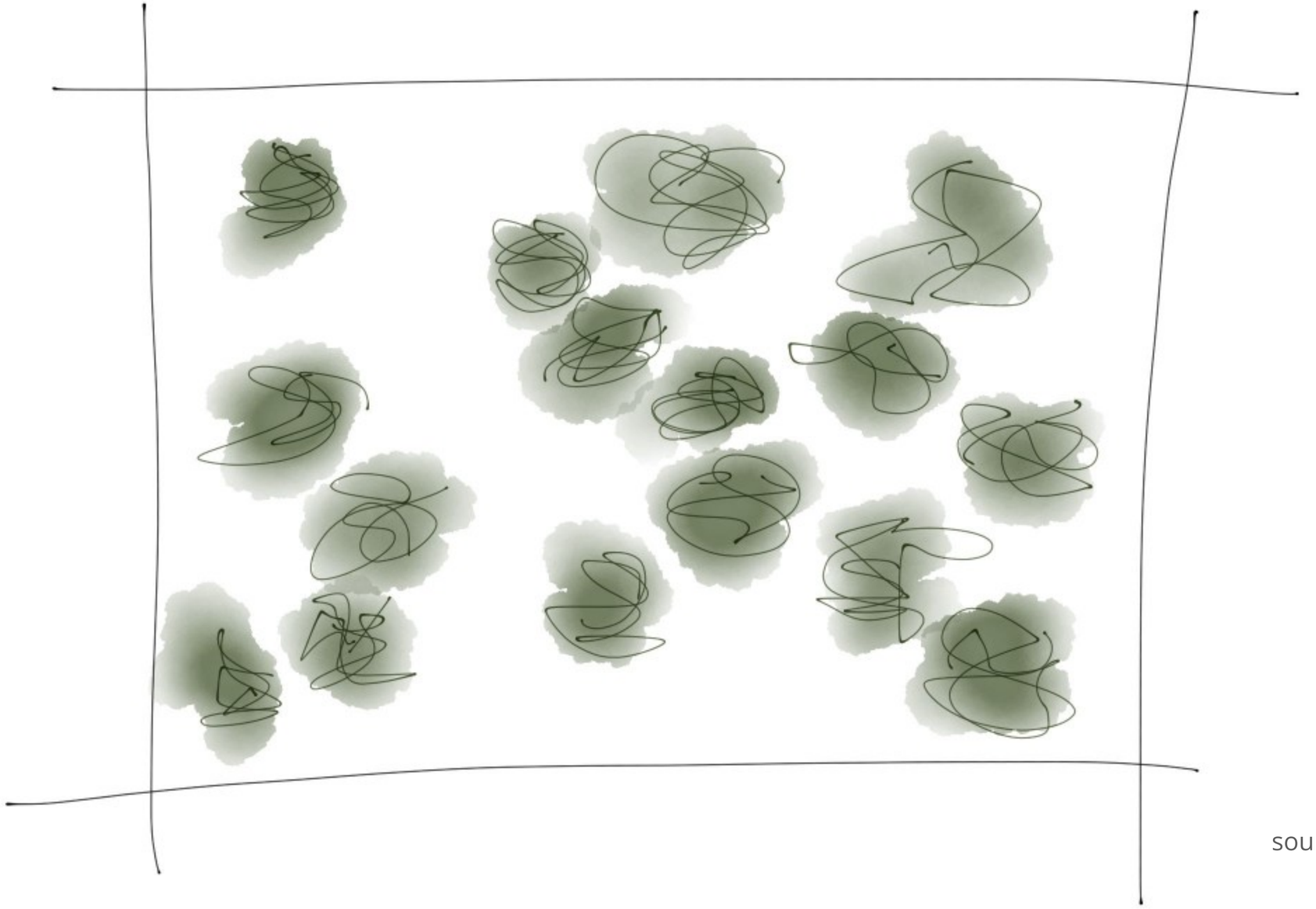
source: https://ronjeffries.com



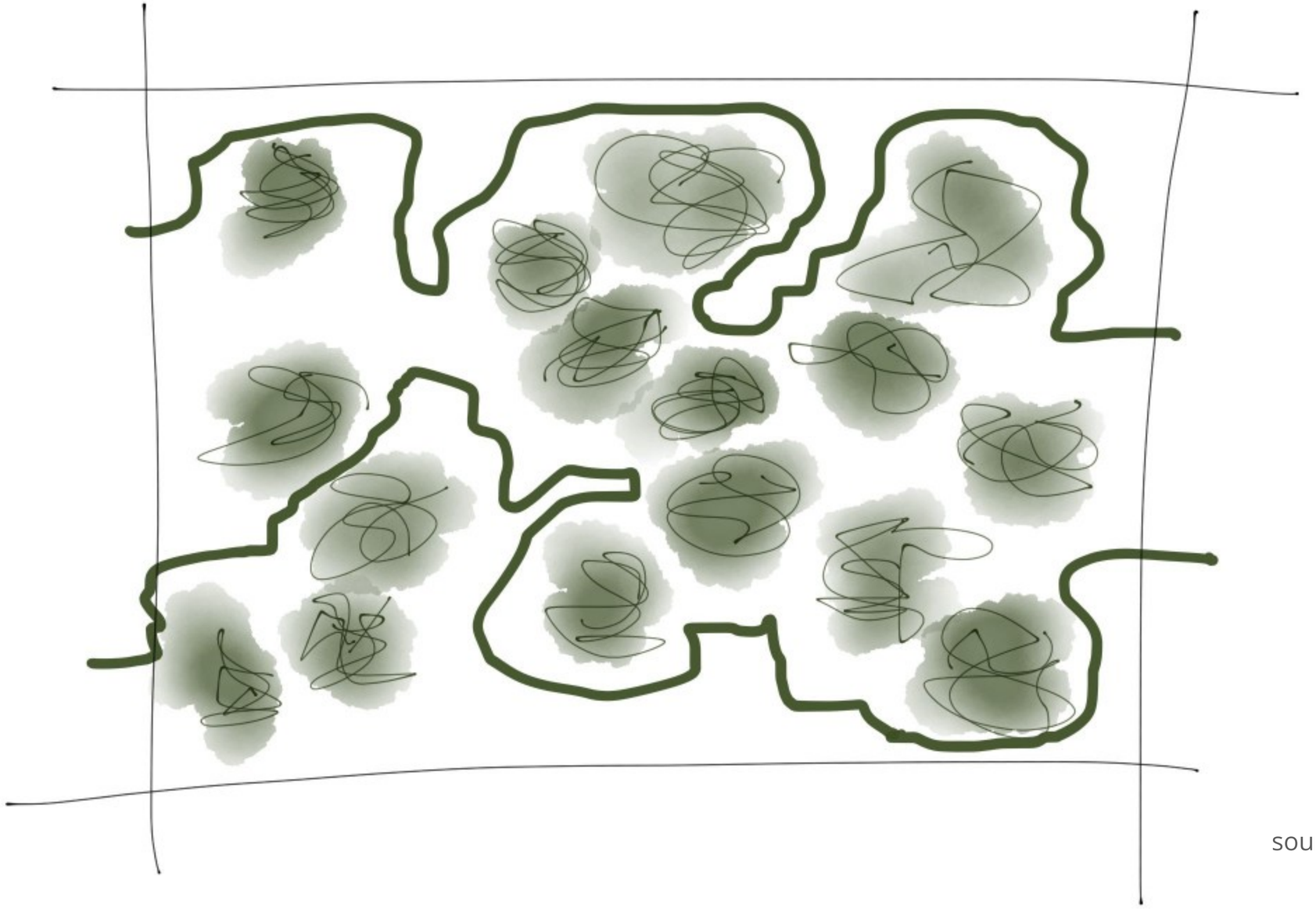
source: https://ronjeffries.com



source: https://ronjeffries.com



source: https://ronjeffries.com



source: https://ronjeffries.com

Defining Software Entropy

goto;

- A **composite** measure of disorder that subsumes **qualitative** and **quantitative** measures.
  – *Saleem Siddiqui*

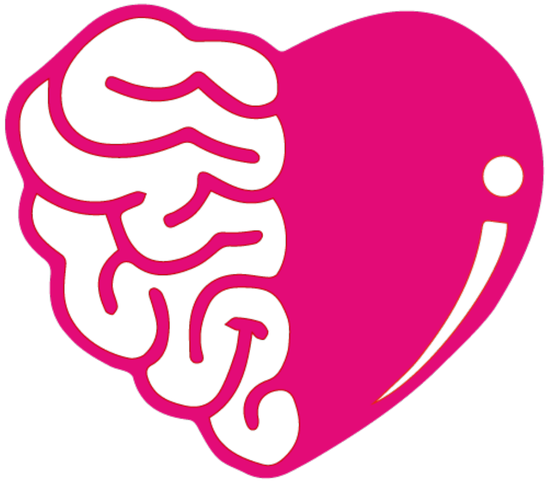
Defining Software Entropy

goto;

Quantitative measures:

- Size (LOC, Num-files, Num-deps)
- Volatility
- Cyclomatic complexity
- Coupling and Instability
- Cohesion: LCOM, TCC, LCC

Defining Software Entropy



Qualitative measures:

- Cognitive load for new developers
- Conformance to the “real” domain

Why does entropy increase?

goto;

Why does entropy increase?

1. Dependency Forest

Dependency Forest

goto;

- Too many dependencies
- Progressive lack of control with transitive dependencies

Dependency Forest

goto;

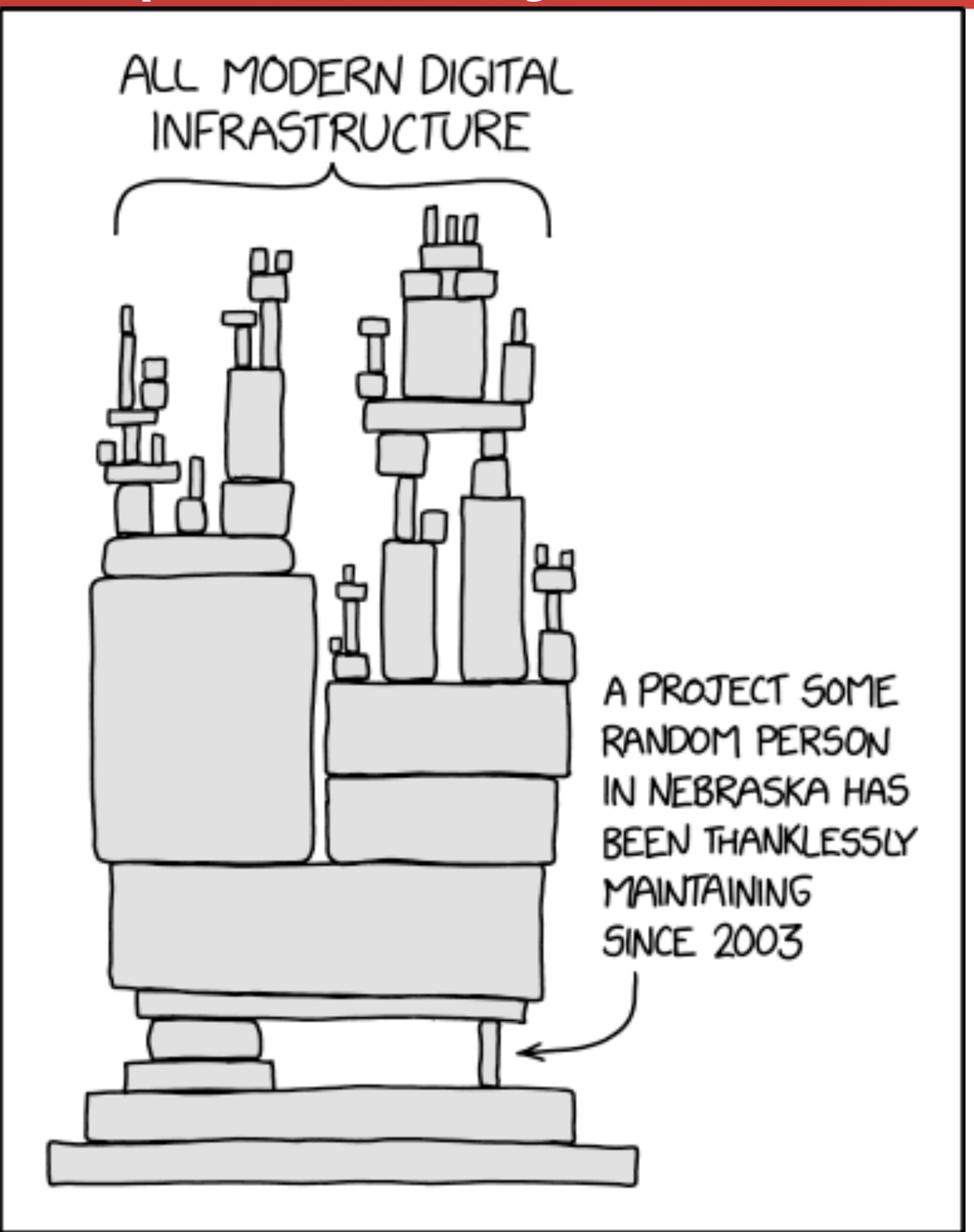
```
saleem@Saleems-MacBook-Air temp % npx create-react-app my-app >/dev/null
saleem@Saleems-MacBook-Air temp % cd my-app
saleem@Saleems-MacBook-Air my-app % npm ls --all | wc -l
[redacted]
saleem@Saleems-MacBook-Air my-app %
```

Dependency Forest

goto;

```
saleem@Saleems-MacBook-Air temp % npx create-react-app my-app >/dev/null
saleem@Saleems-MacBook-Air temp % cd my-app
saleem@Saleems-MacBook-Air my-app % npm ls --all | wc -l
    3114
saleem@Saleems-MacBook-Air my-app %
```

Dependency Forest



That project could be left pad ...

How one programmer broke the internet by deleting a tiny piece of code

leftpad.js package.json

```
1  module.exports = leftpad;
2  function leftpad (str, len, ch) {
3    str = String(str);
4    var i = -1;
5    if (!ch && ch !== 0) ch = ' ';
6    len = len - str.length;
7    while (++i < len) {
8      str = ch + str;
9    }
10   return str;
11 }
12
```

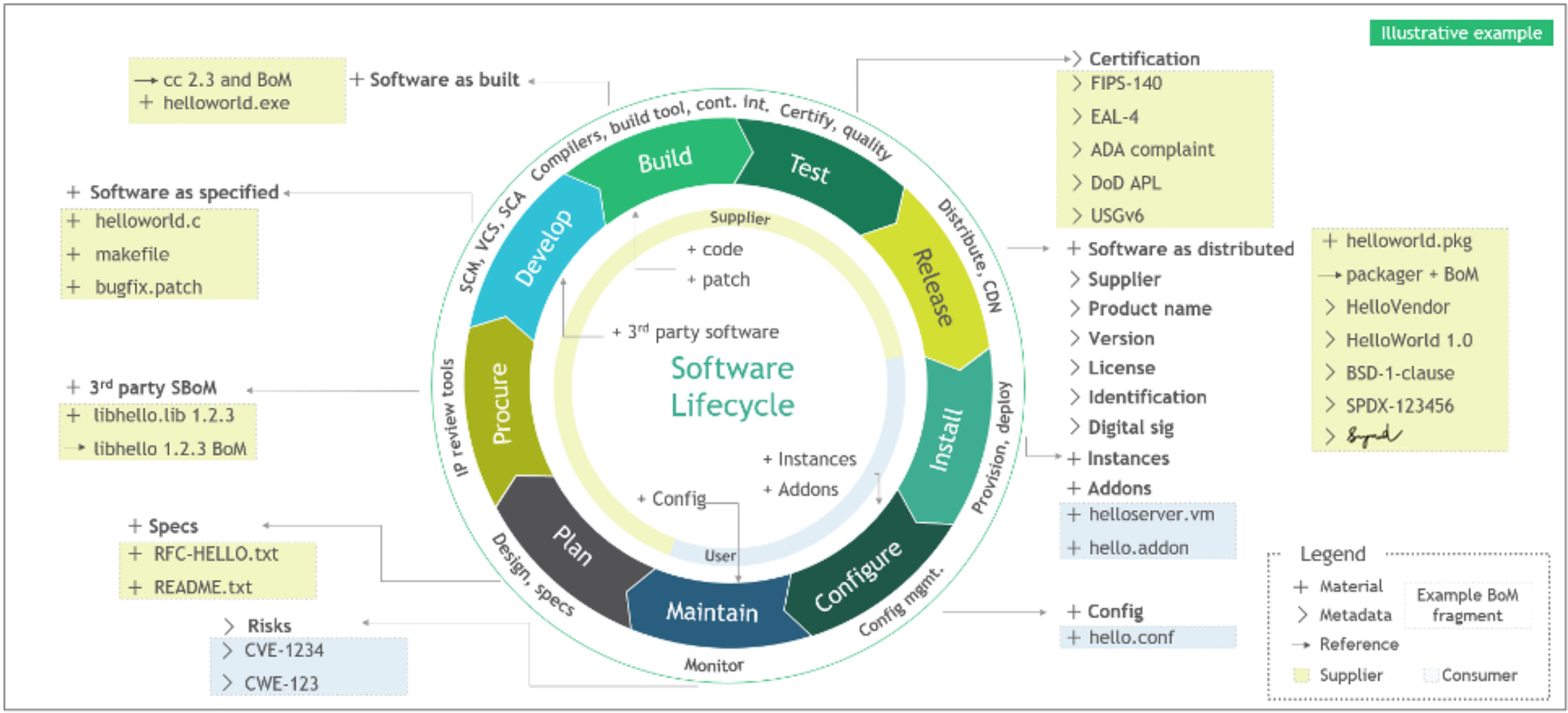
Dependency Forest

goto;

- Create an SBOM - Software Bill of Material
- Pin your dependencies - don’t be permissive with ~ and ^
- Enforce dependencies through fitness functions

SBOM

goto;


Illustrative example
→ cc 2.3 and BoM
+ helloworld.exe
+ Software as built
+ Software as specified
+ helloworld.c
+ makefile
+ bugfix.patch
+ 3rd party SBoM
+ libhello.lib 1.2.3
→ libhello 1.2.3 BoM
+ Specs
+ RFC-HELLO.txt
+ README.txt
> Risks
> CVE-1234
> CWE-123
> Certification
> FIPS-140
> EAL-4
> ADA complaint
> DoD APL
> USGv6
+ Software as distributed
> Supplier
> Product name
> Version
> License
> Identification
> Digital sig
+ Instances
+ Addons
+ helloserver.vm
+ hello.addon
+ Config
+ hello.conf
+ helloworld.pkg
→ packager + BoM
> HelloVendor
> HelloWorld 1.0
> BSD-1-clause
> SPDX-123456
> Sigrid
Build
Test
Release
Install
Configure
Maintain
Plan
Procure
Develop
Compilers, build tool, cont. int.
Certify, quality
Distribute, CDN
Provision, deploy
Config mgmt.
Monitor
Design, specs
IP review tools
SCM, VCS, SCA
Supplier
+ code
+ patch
+ 3rd party software
Software Lifecycle
+ Instances
+ Addons
+ Config
User
Legend
+ Material
> Metadata
→ Reference
Example BoM fragment
Supplier
Consumer

Department of Commerce
The Minimum Elements for an SBOM

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Architecture Fitness Functions

goto;

```
describe "Layering" do
  it “must adhere to prescribed layering" do
    expect(dependencies_from(ado).to(service)).to be(0)
  end
end
```

Why does entropy increase?

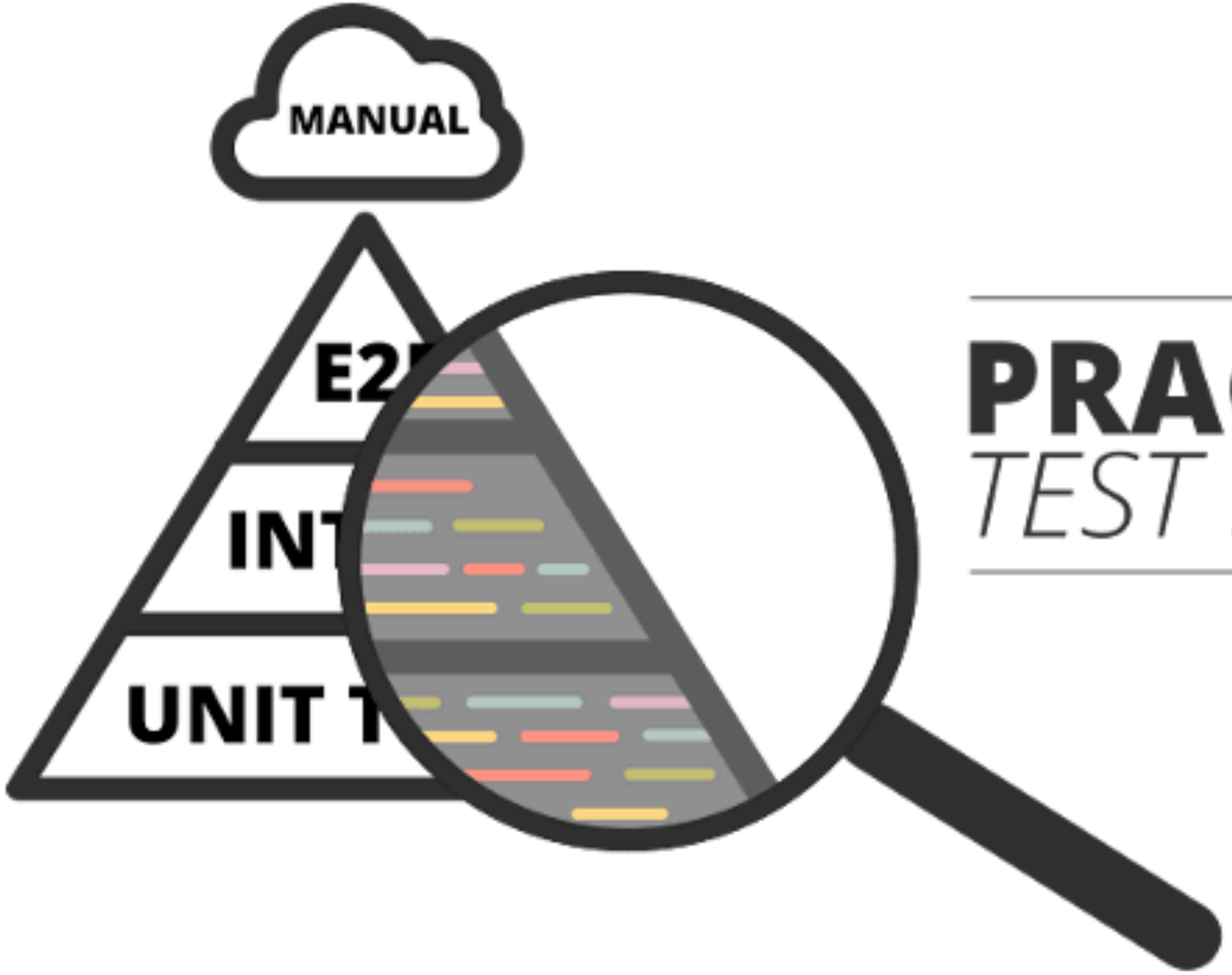
goto;

Why does entropy increase?

2. Lopsided Test Strategy

Lopsided Test Strategy

goto;



THE
PRACTICAL
TEST PYRAMID

source: https://martinfowler.com

Lopsided Test Strategy

goto;

```
Scenario: Shipping and Billing Address
    Given the page "Checkout" is visible
    When I click the checkbox “Same as Shipping Address"
    Then “Billing Address” should be hidden
```

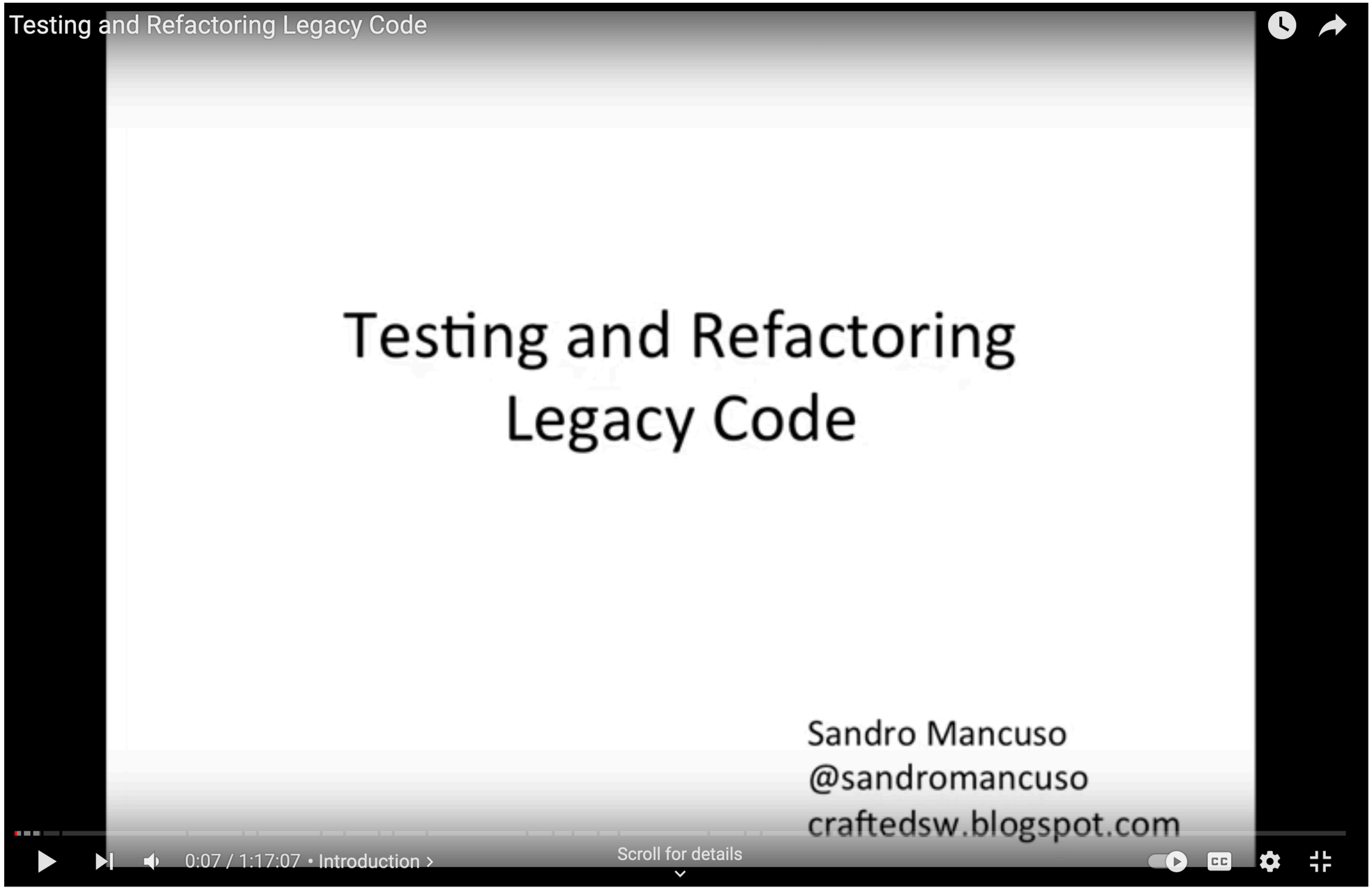
Lopsided Test Strategy

goto;

```
@Test
@DisplayName(“should use billing address as shipping address”)
void testSameAddresses() {
  Customer c = new CustomerBuilder()
       .withShipping(“123 Main St.”)
       .withBillingSameAsShipping(true).build();
  assertThat(
       c.getShippingAddress(), equalTo(c.getBillingAddress()));
}
```

Lopsided Test Strategy

goto;



source:
youtube.com/watch?v=_NnElPO5BU0

Why does entropy increase?

goto;

Why does entropy increase?

3. Progressive Test Anemia

Progressive Test Anemia

goto;

Anemia is a problem of not having enough healthy red blood cells or hemoglobin to carry oxygen to the body's tissues.
There are many forms of anemia. Each has its own cause. Anemia can be short term or long term. It can range from mild to severe. Anemia can be a warning sign of serious illness.

source: source: https://www.mayoclinic.org/diseases-conditions/anemia/symptoms-causes/syc-20351360

Progressive Test Anemia

goto;

Test anemia is a problem of not having enough **healthy green tests** to carry the burden of finding issues. There are many forms of test anemia. Each has its own cause. Test anemia can be short term or long term. It can range from mild to severe. Test anemia can be a warning sign of **serious software illness**.

Progressive Test Anemia

goto;

```
class PublicClass {
  public void realMethod(){
    //production code
  }

  public static void fakeMethod(){
    integer i = 0;
    i++;
    i++;
    //repeat the i++ hundred of times
  }
}

class PublicClassTest{

  @Test void testMethod (){
     PublicClass.fakeTest();
  }
}
```

Adapted from: salesforce.stackexchange.com/questions/25892/the-most-sneaky-way-to-increase-your-code-coverage

Progressive Test Anemia

goto;

```
class PublicClass {
  public void realMethod(){
    //production code
  }

  public static void fakeMethod(){
    integer i = 0;
    i++;
    i++;
    //repeat the i++ hundred of times
  }
}

class PublicClassTest{

  @Test void testMethod (){
     PublicClass.fakeTest();
  }
}
```

Adapted from: salesforce.stackexchange.com/questions/25892/the-most-sneaky-way-to-increase-your-code-coverage

Progressive Test Anemia

goto;

Fix the underlying problem, don't *just* "fix the broken build"

Progressive Test Anemia

goto;

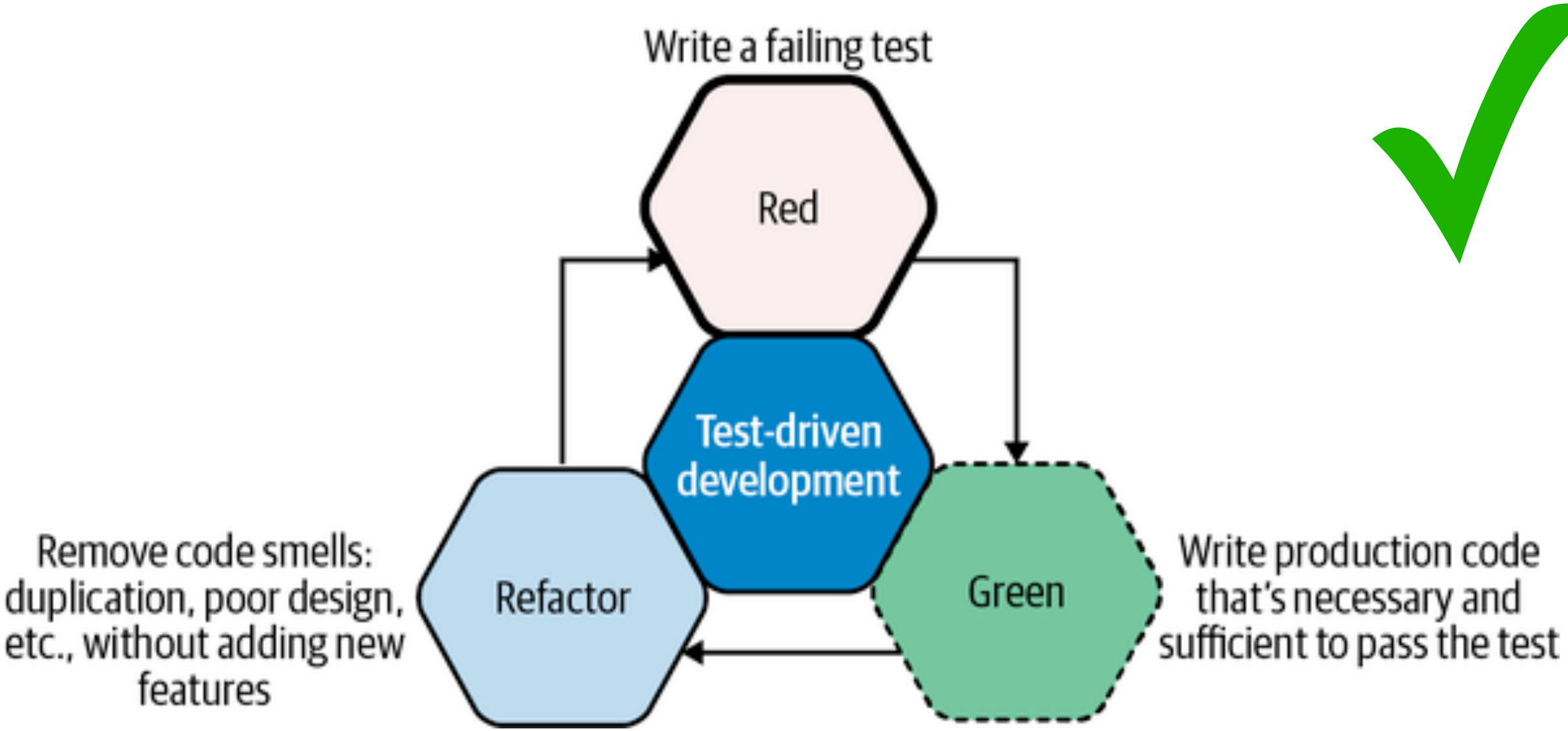
Use test-driven development for production code

Progressive Test Anemia

goto;

Progressive Test Anemia

goto;



Why does entropy increase?

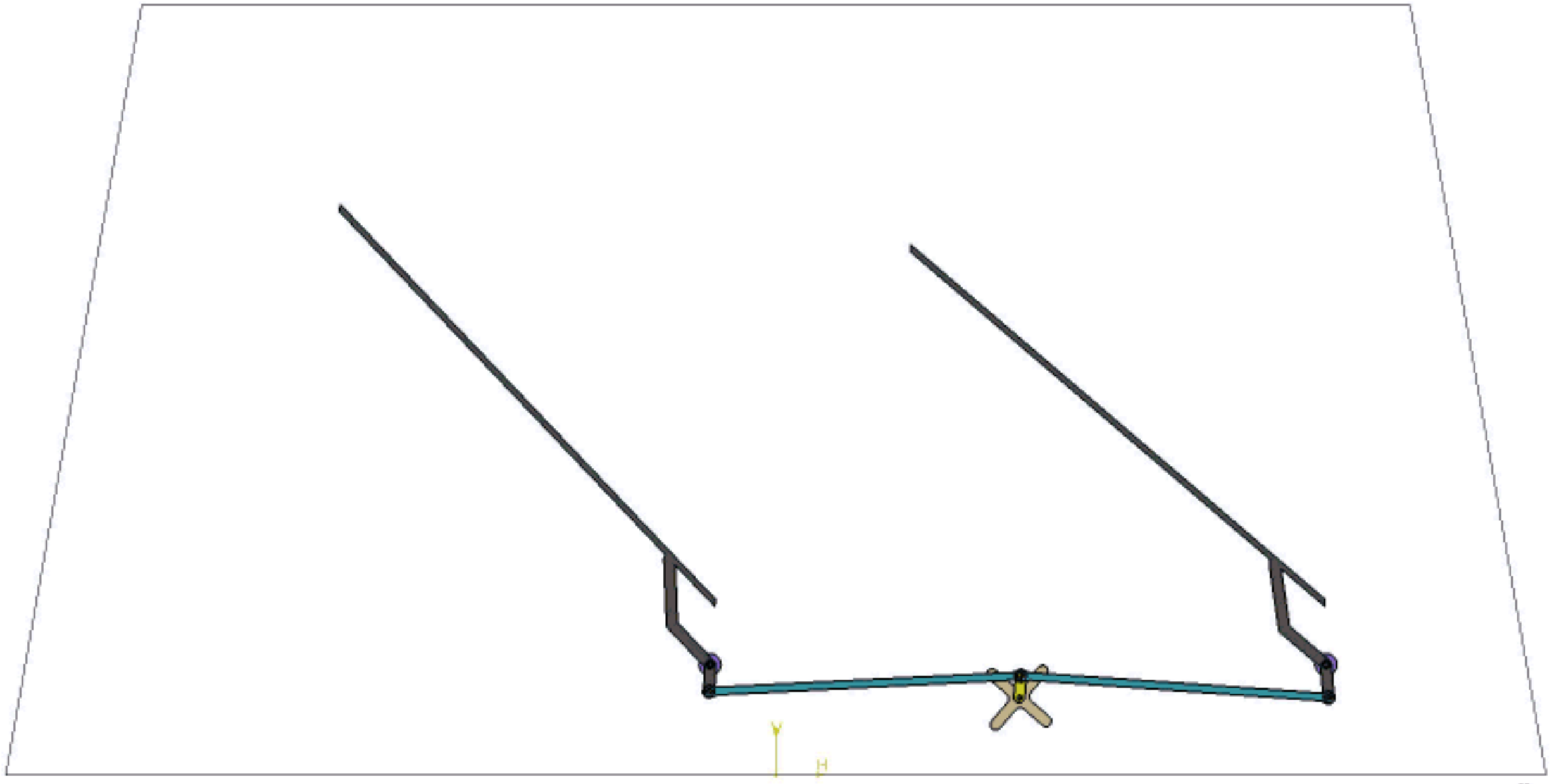
goto;

Why does entropy increase?

4. Over-engineering

Overengineering

goto;

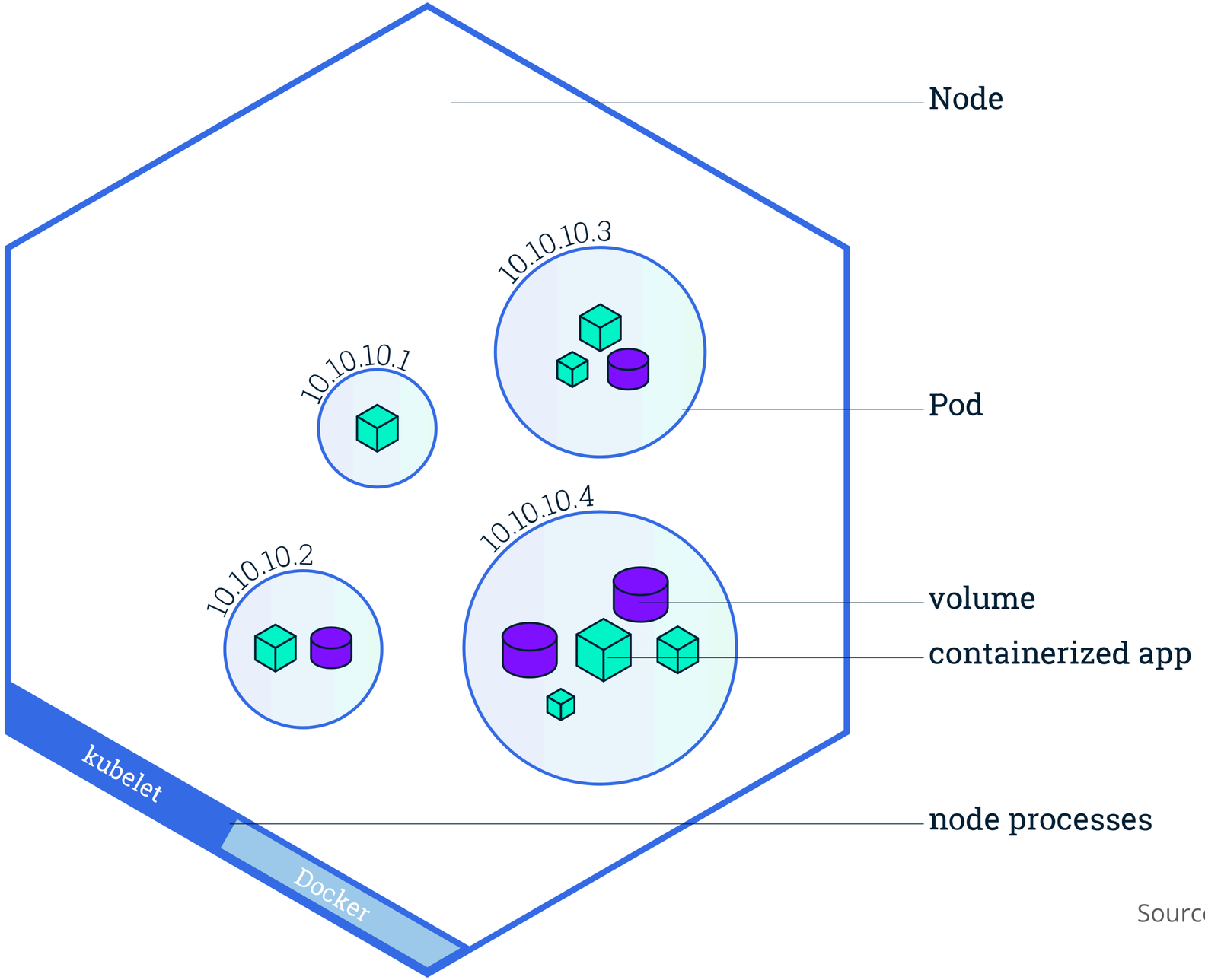


Overengineering

goto;

Overengineering

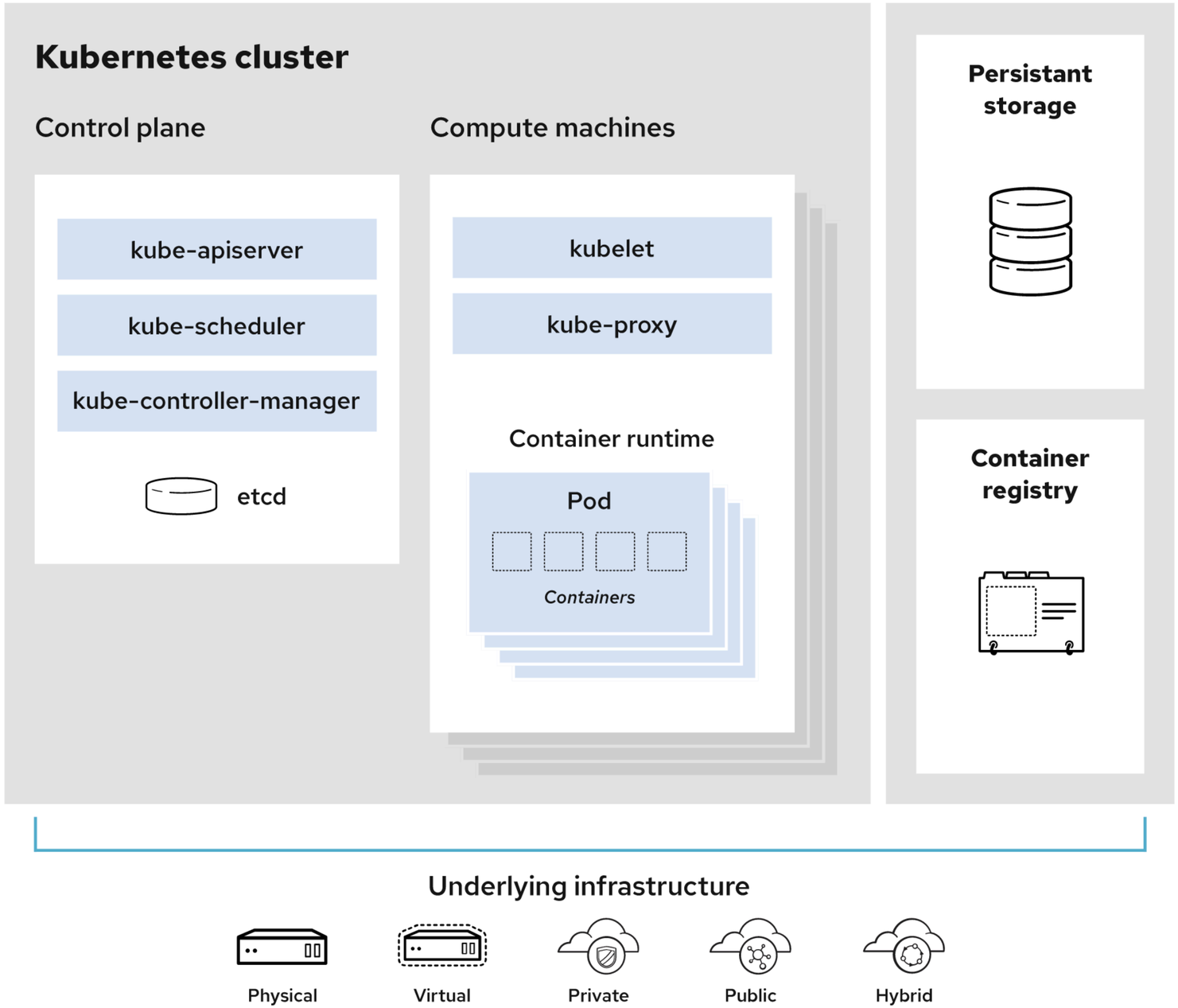
goto;



Source: cloudfront.net

Overengineering

goto;



Overengineering

goto;

Simplicity – the art of maximizing the amount of work **not** done

Overengineering

goto;

Satisficing – a decision making heuristic that emphasizes the **total** cost of the decision, including the time needed to make it

Overengineering

goto;

Why does entropy increase?

goto;

Why does entropy increase?

5. Stuff we cannot foresee

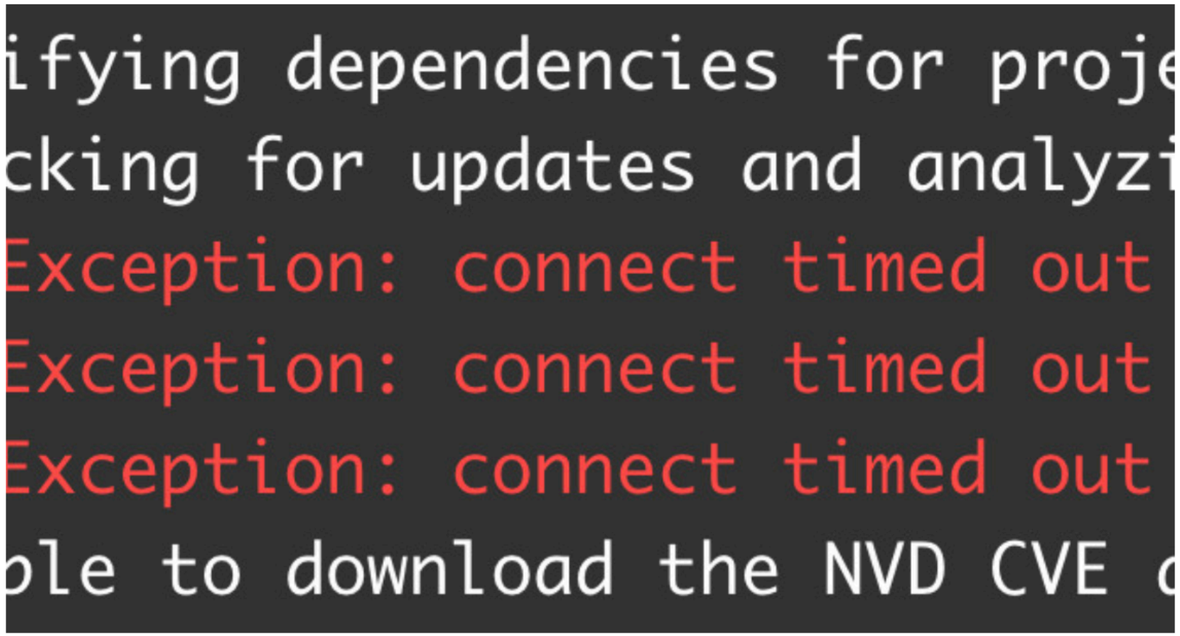
Stuff we cannot foresee

goto;

How about a federal government shutdown?

Stuff we cannot foresee

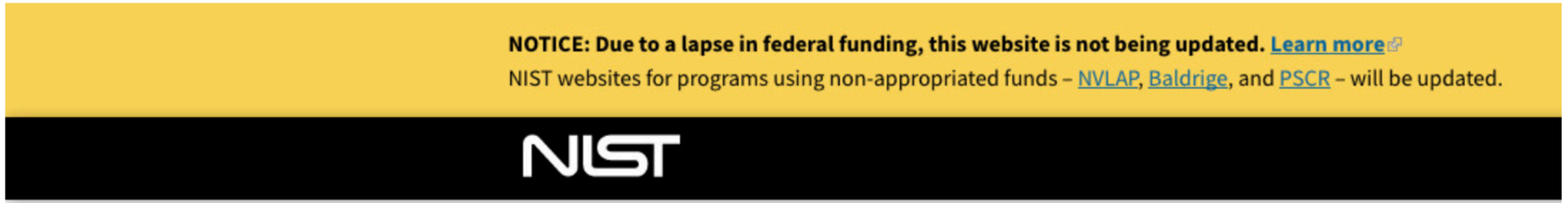
goto;



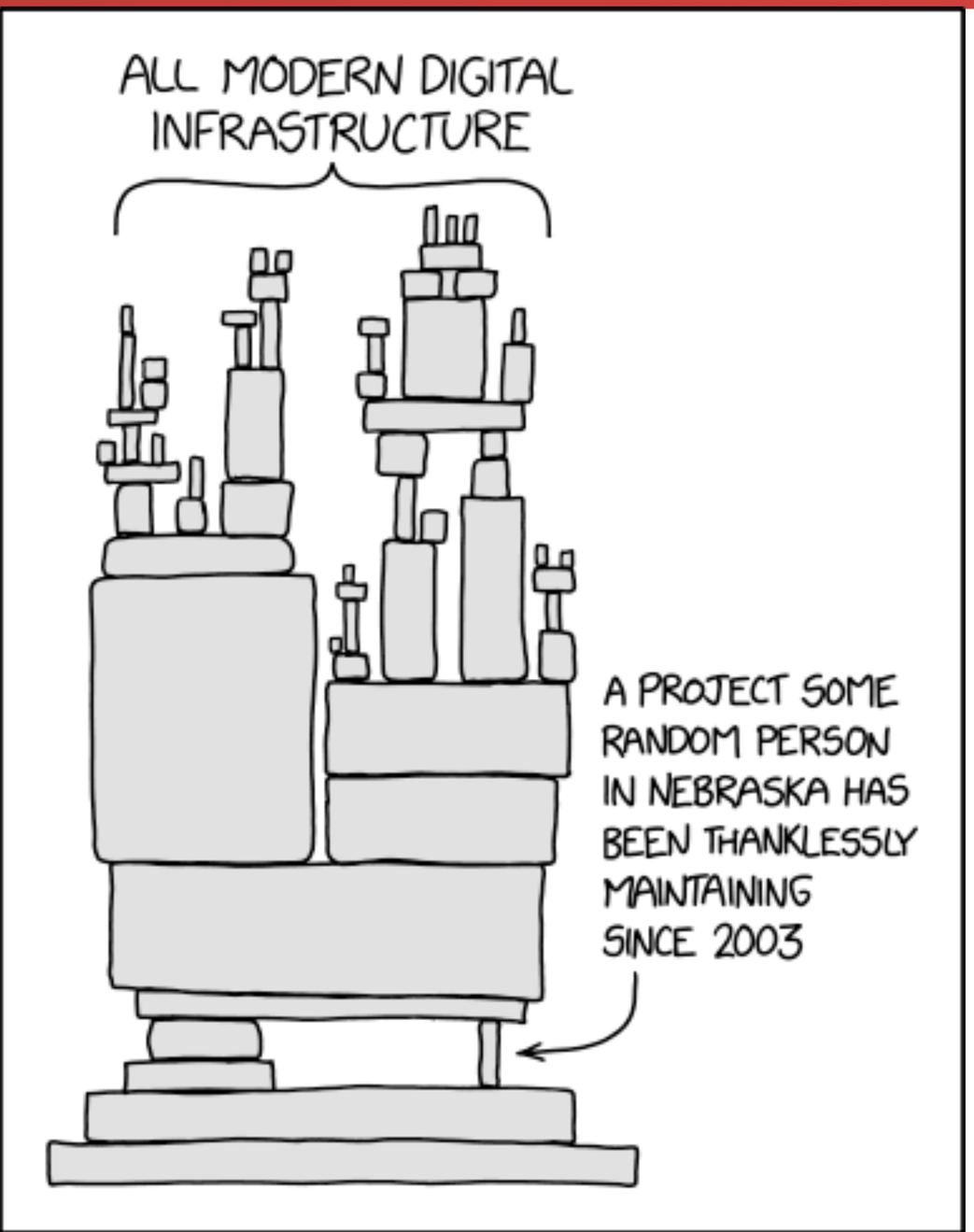
Images by author

The US federal government shutdown broke my software (seriously)

Source: https://www.linkedin.com/pulse/us-federal-government-shutdown-broke-my-software-saleem-siddiqui/



Stuff we cannot foresee



That dependency could be the NIST CVE database ...

goto;

Why does entropy increase?

5-α. Stuff we ***refuse*** to foresee

Stuff we refuse to foresee

goto;

```
Welcome to Node.js v20.1.0.
Type ".help" for more information.
> const arr = [1,2,3,]
undefined
> arr
[ 1, 2, 3 ]
> JSON.parse("[1,2,3,]")
```

Stuff we refuse to foresee

goto;

```
Welcome to Node.js v20.1.0.
Type ".help" for more information.
> const arr = [1,2,3,]
undefined
> arr
[ 1, 2, 3 ]
> JSON.parse("[1,2,3,]")
Uncaught SyntaxError: Unexpected token ']', "[1,2,3,]" is not valid JSON
> 
```

Stuff we refuse to foresee

Defend against the horrors that you can - you may be surprised how long a list that is!

Why does entropy increase?

goto;

1. Dependency Forest
2. Progressive Test Anemia
3. Lopsided Test Strategy
4. Over-engineering

5-α. Stuff we ***refuse*** to foresee

Thank you!

Don’t forget to
vote for this session
in the **GOTO Guide app**

goto;

goto;

GOTO **CHICAGO 2023**

May 22-24, 2023

@s2il

linkedin.com/in/ssiddiqui