

# THE ASSURANCE RECIPE: FACILITATING ASSURANCE PATTERNS

 **ESQuaReD**

JUSTIN FIRESTONE, UNIVERSITY OF NEBRASKA - LINCOLN

AND MYRA COHEN, IOWA STATE UNIVERSITY

FUNDING PROVIDED IN PART BY THE NATIONAL INSTITUTE OF JUSTICE, GRANT 2016-R2-CX-0023  
AND NATIONAL SCIENCE FOUNDATION GRANT CCF-1745775.

UNIVERSITY OF  
**Nebraska**  
Lincoln®

**IOWA STATE UNIVERSITY**  
OF SCIENCE AND TECHNOLOGY

# COMMON DOMAINS FOR ASSURANCE CASES

- OFFSHORE DRILLING
- NUCLEAR POWER
- AVIONICS
- AUTOMOTIVE SOFTWARE
- RAILROADS

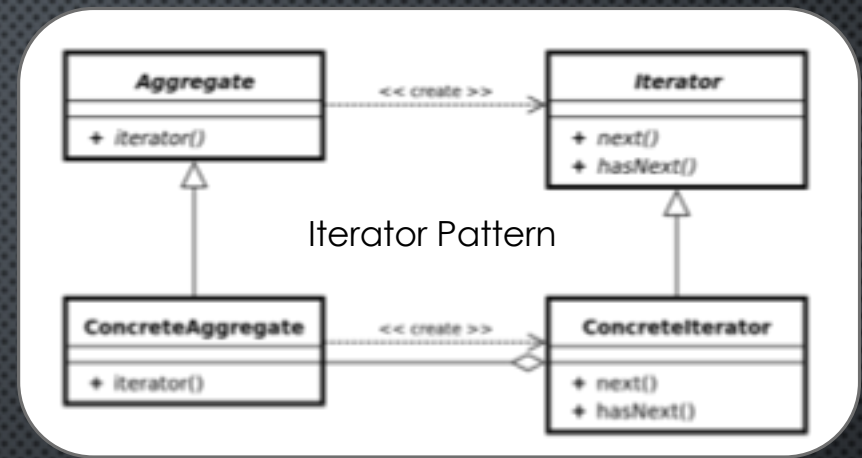


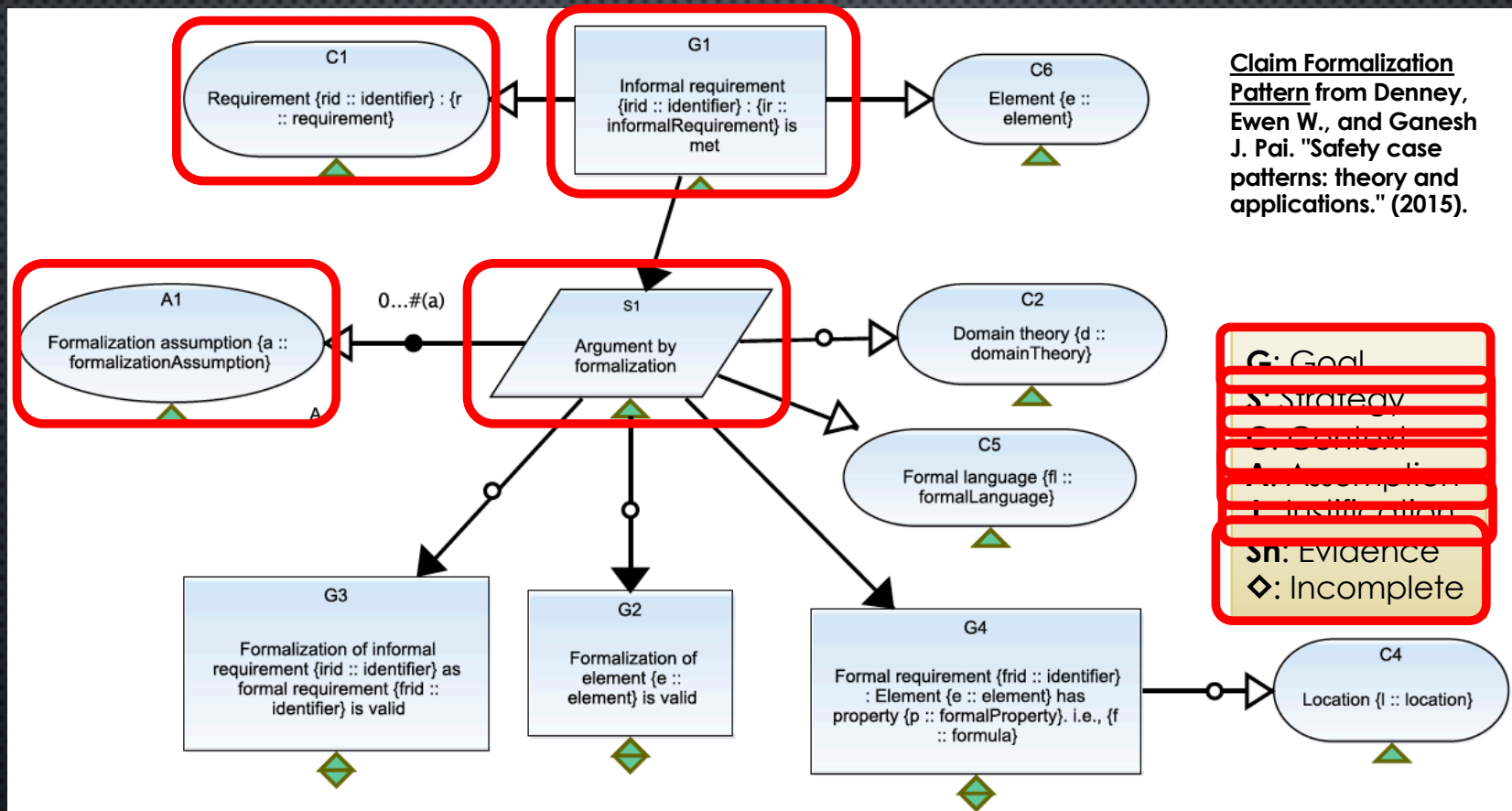
Piper Alpha (North Sea) disaster of 1986, with 167 deaths



# ASSURANCE PATTERNS

- COMMON PROBLEMS HAVE COMMON SOLUTIONS
- RESEARCHERS HAVE BEEN DEVELOPING PATTERNS FOR REUSE AND STANDARDIZATION
- ASSURANCE PATTERNS ARE LIKE CODING **PATTERNS** AND **ANTI-PATTERNS**
  - ABSTRACT META-DESCRIPTIONS
  - EVOLVING TOWARD BEST PRACTICES (CONSIDER THE ITERATOR PATTERN)



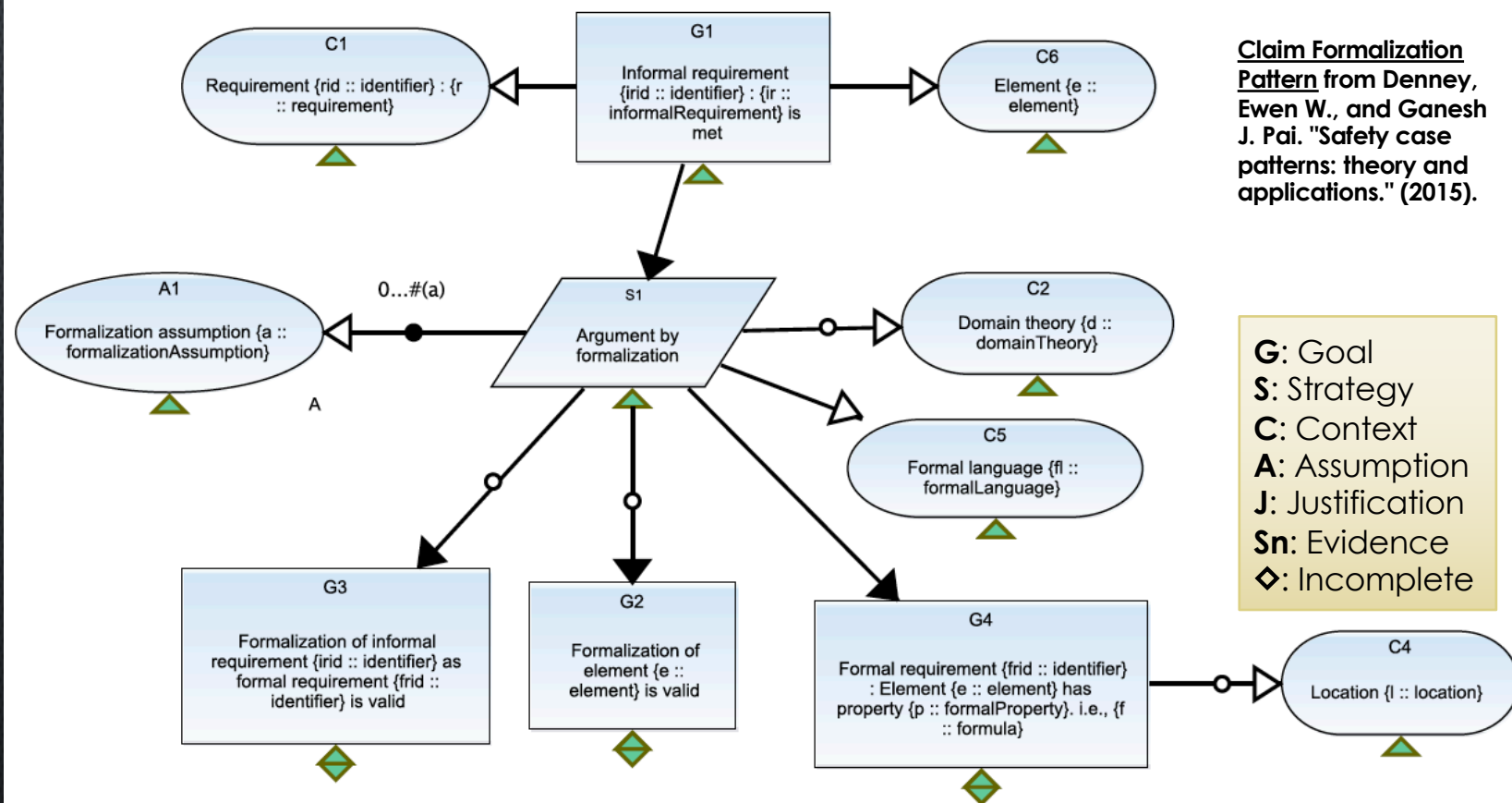




# CHALLENGE

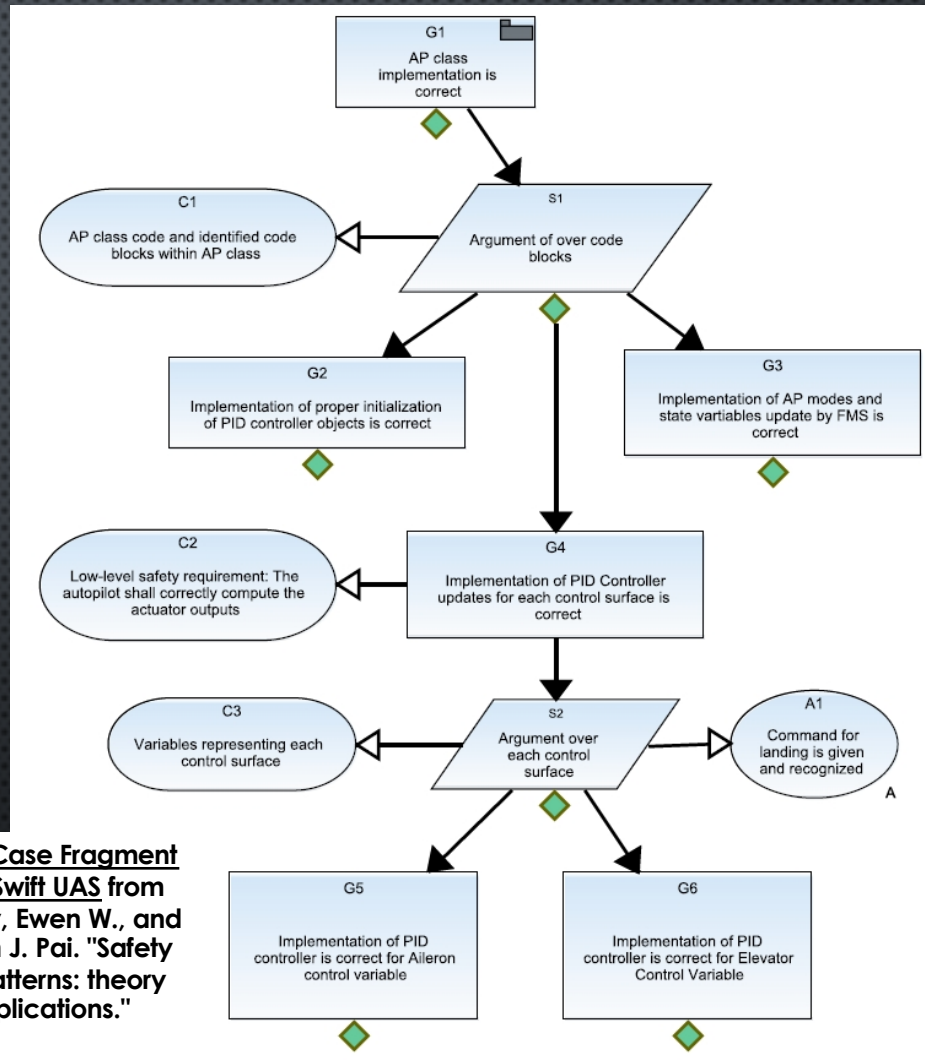
- PATTERNS ARE USEFUL GUIDANCE FOR EXPERTS, BUT
  - THEY ARE VERY ABSTRACT
  - THEY REQUIRE DOMAIN EXPERTISE AND SPECIFIC KNOWLEDGE
- HOW WOULD A NON-EXPERT OR SOMEONE FROM A NON-TRADITIONAL DISCIPLINE KNOW HOW TO USE THEM?







# INSTANTIATION OF CLAIM FORMALIZATION PATTERN FOR UAS



**Safety Case Fragment  
for the Swift UAS from  
Denney, Ewen W., and  
Ganesh J. Pai. "Safety  
case patterns: theory  
and applications."  
(2015).**

# OUR EXPERIENCE

- USERS NEW TO ASSURANCE CASES CONFUSE TERMINOLOGY AND STRUCTURE
  - ASSUMPTIONS CONFUSED WITH JUSTIFICATIONS AND CONTEXTS
  - GOALS CONFUSED WITH EVIDENCE AND ARGUMENTS NEEDED TO SUPPORT THEM
- CONCLUSION: MORE STRUCTURE AND LESS FREEDOM WOULD HELP
- INSPIRED BY **ASSURANCE PATTERNS**, WE PRESENT **ASSURANCE RECIPES**

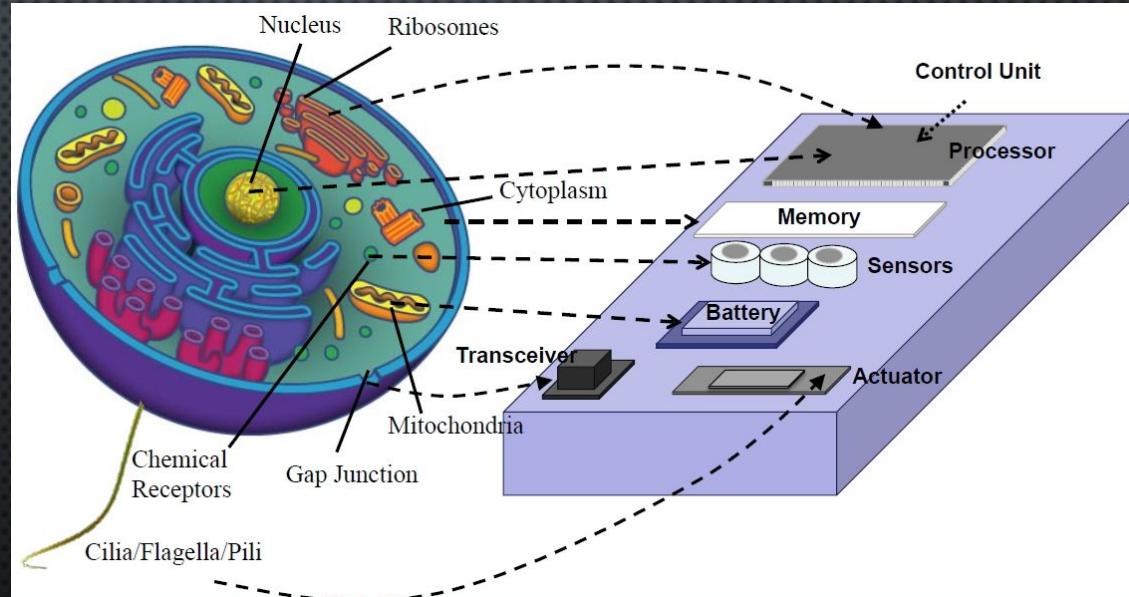


# PRESENTATION OUTLINE

- MOTIVATION
- BACKGROUND ON SYNTHETIC BIOLOGY
- PRE-STUDY
- THE ASSURANCE RECIPE
- FEASIBILITY STUDY
- CONCLUSION

# EMERGING DOMAIN: SYNTHETIC BIOLOGY (SB)

CELLS ARE LIKE  
COMPUTATIONAL  
DEVICES

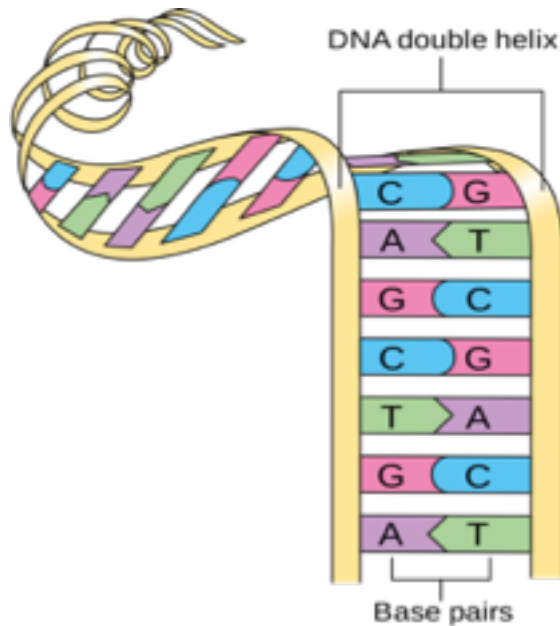


I. F. Akyildiz, M. Pierobon, S. Balasubramaniam and Y. Koucheryavy, "The Internet of Bio-Nano Things," in IEEE Communications Magazine, vol. 53, no. 3, pp. 32-40, March 2015.



# LIFE AS CODE

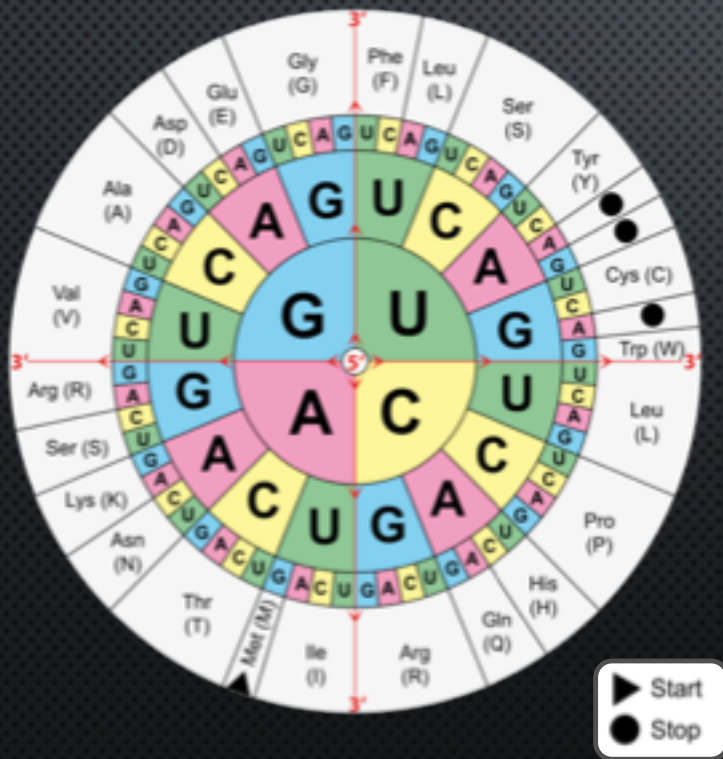
## NUCLEOBASES AS MACHINE CODE



= 00001000

# LIFE AS CODE

## PEPTIDES AS ASSEMBLY CODE

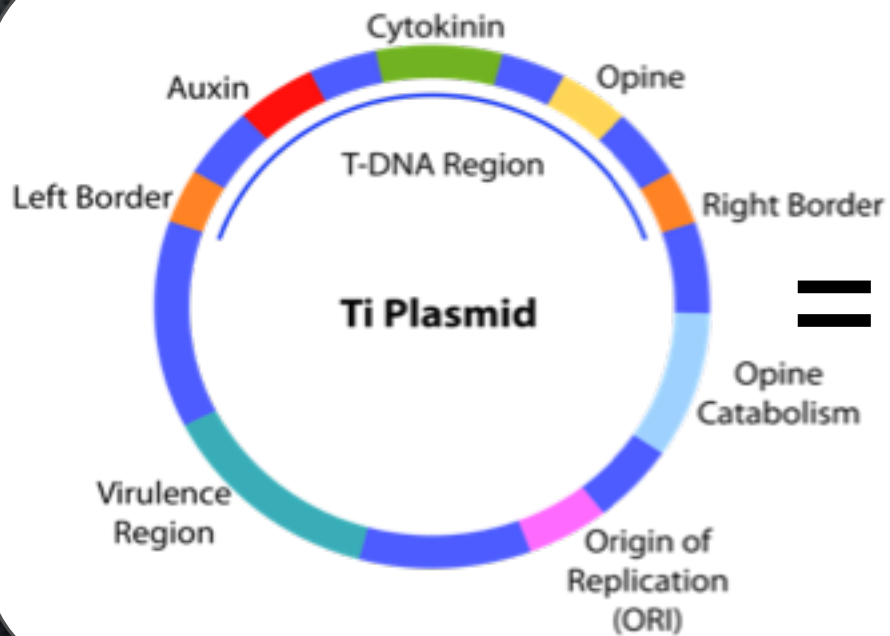


=  
MOV AL, 1h  
MOV CL, 2h  
MOV DL, 3h



# LIFE AS CODE

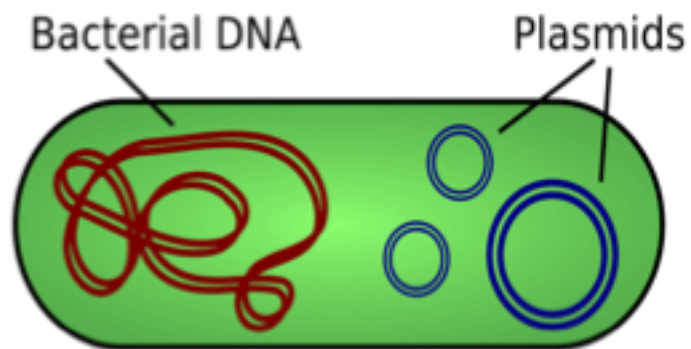
## PLASMIDS AS METHODS



```
main()  
{  
    printf("?");  
}
```

# LIFE AS CODE

## CELLS AS SOFTWARE



=





# LIFE AS CODE

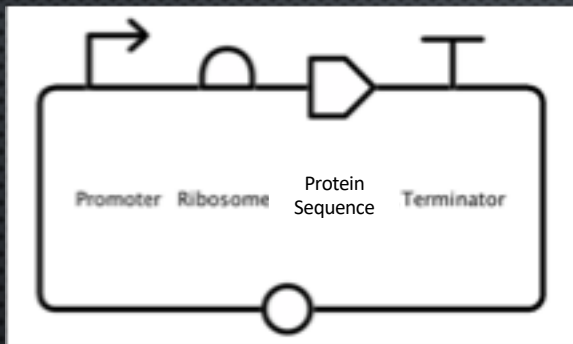
## ORGANISMS AS SYSTEMS



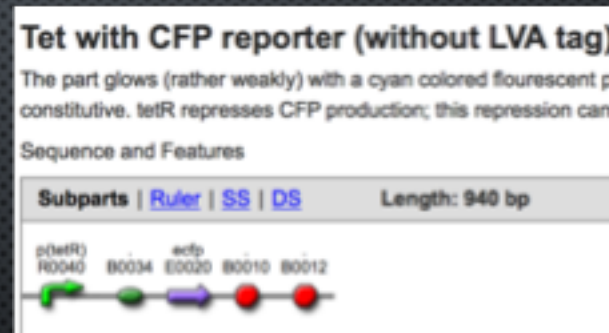
=



# PROGRAMMING LIFE



Program using SBOL [1]



Reporter from iGEM Registry [2]

[1] [sbolstandard.org](http://sbolstandard.org)

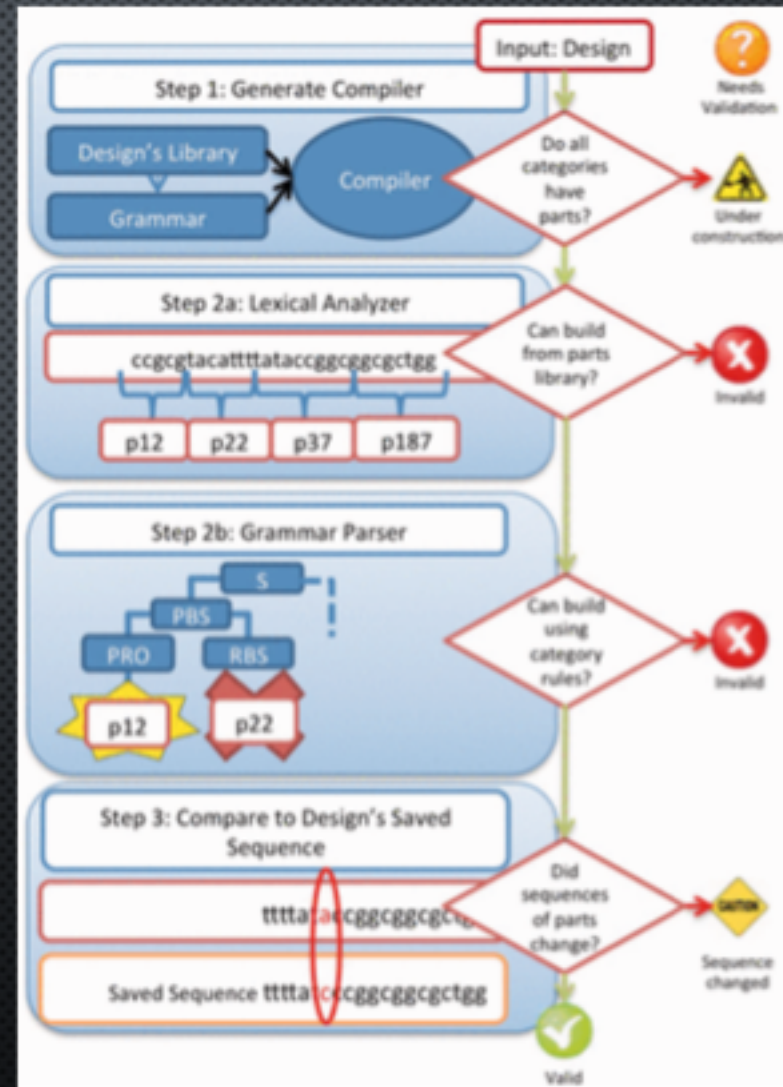
[2] [parts.igem.org/Part:BBa\\_I13600](http://parts.igem.org/Part:BBa_I13600)



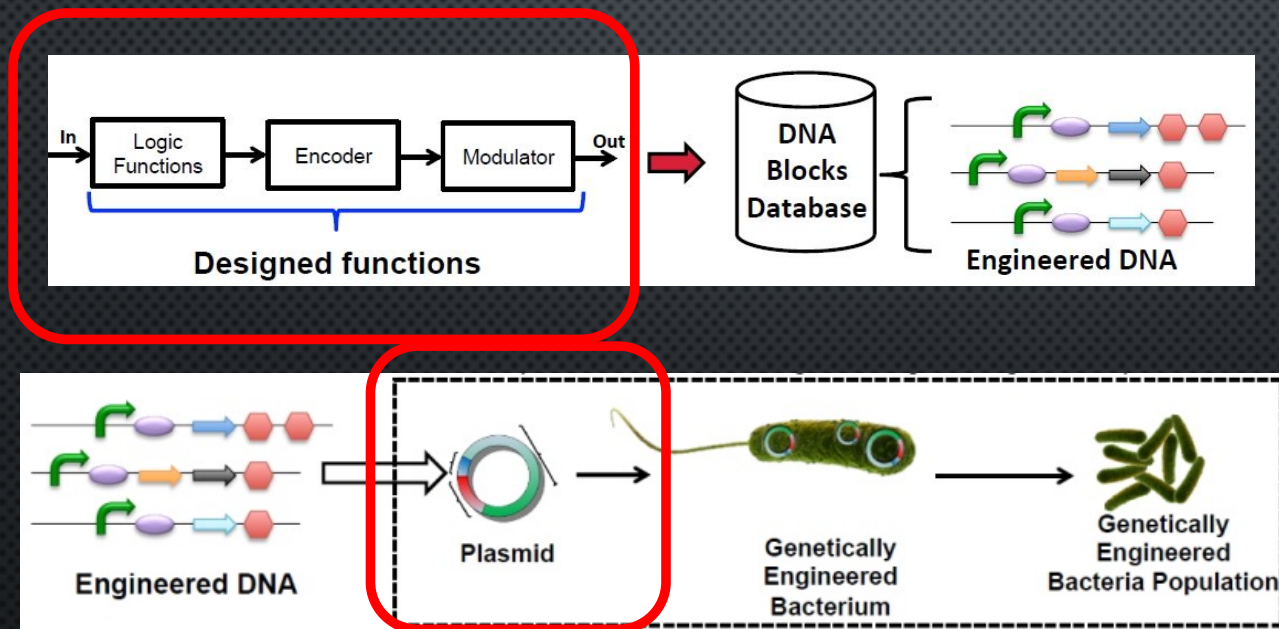
# PROGRAMMING LIFE

- DNA COMPILER
- DNA ANALYZER
- DNA PARSER

Mandy L. Wilson, Sakiko Okumoto, Laura Adam, Jean Peccoud; Development of a domain-specific genetic language to design *Chlamydomonas reinhardtii* expression vectors, *Bioinformatics*, Volume 30, Issue 2, 15 January 2014, Pages 251–257



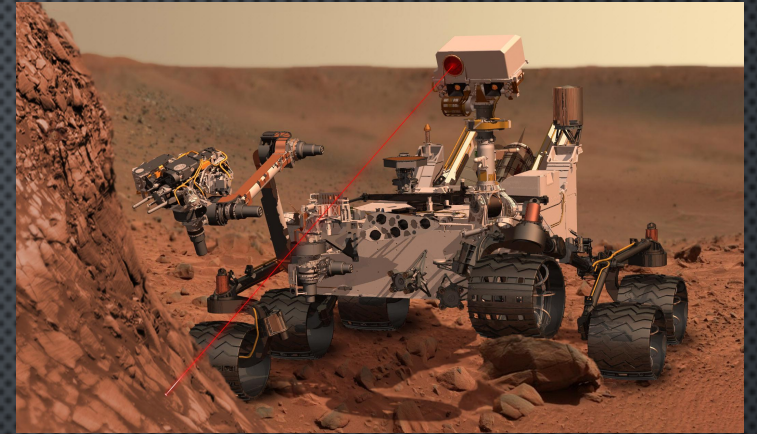
# SB ALLOWS ENGINEERED CELLS



- IMPROVE EXISTING BEHAVIOR
- EXHIBIT NOVEL BEHAVIOR



## POTENTIAL SB USES



- DETECT WHETHER MEAT OR PRODUCE HAS SPOILED
- IMPROVE SOIL QUALITY AND MITIGATE POLLUTION
- PRODUCE CLEAN BIOFUELS
- MAKE INTELLIGENT DRUGS TARGETING SPECIFIC BODY PARTS
- TERRAFORM MARS FOR COLONIZATION

# SB IS A SAFETY-CRITICAL ENGINEERING DISCIPLINE

- SYNTHETICALLY ENGINEERED BIOLOGICAL ORGANISMS (SEBOs) CAN CAUSE HARM TO LIFE AND THE ENVIRONMENT
- SOFTWARE ENGINEERING PRINCIPLES CAN APPLY TO SEBOS
- CAN WE “CERTIFY” SEBOs?



## Whatever Happened to the Glowing Plant Kickstarter?

The project seized on one of the most romantic fantasies of synthetic biology.

SARAH ZHANG | APR 20, 2017 | SCIENCE

20

[theatlantic.com/science/archive/2017/04/whatever-happened-to-the-glowing-plant-kickstarter/523551/](http://theatlantic.com/science/archive/2017/04/whatever-happened-to-the-glowing-plant-kickstarter/523551/)



# THE INTERNATIONAL GENETICALLY ENGINEERED MACHINES (iGEM) COMPETITION



[http://2017.igem.org/wiki/images/f/ff/HQ\\_About2017\\_1.png](http://2017.igem.org/wiki/images/f/ff/HQ_About2017_1.png)



# THE iGEM COMPETITION

- HELD EVERY YEAR AT MIT IN BOSTON
- IN 2017: 314 TEAMS FROM 40 COUNTRIES
  - OVER 6,000 STUDENTS (MOSTLY UNDERGRADUATES)
  - THE TEAM FROM GHANA MADE SOME OF THEIR OWN INSTRUMENTS FROM LEGOS
- FOR 2018: 371 TEAMS REGISTERED
- EVERY TEAM GETS A WIKI STUB TO SHARE PROJECT DETAILS (OPEN-SOURCE PHILOSOPHY)
- TEAMS CAN BE AWARDED BRONZE, SILVER, OR GOLD MEDALS, IN ADDITION TO SPECIFIC CATEGORY AWARDS

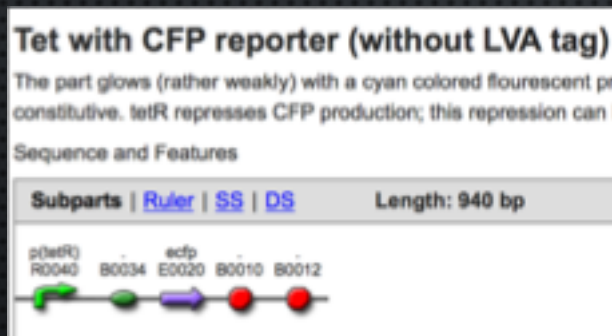


[http://2017.igem.org/wiki/images/f/ff/HQ\\_About2017\\_1.png](http://2017.igem.org/wiki/images/f/ff/HQ_About2017_1.png)



# A SIMPLE SB PROJECT

INTRODUCTORY TEST PROJECT FROM THE  
2017 UNIVERSITY OF NEBRASKA —  
LINCOLN (UNL) INTERNATIONAL  
GENETICALLY ENGINEERED MACHINES  
(IGEM) TEAM



leifeld / dna

[Watch](#) 17
 [Star](#) 32
 [Fork](#) 18

[Code](#)
[Issues](#) 23
 [Pull requests](#) 0
 [Projects](#) 0
 [Insights](#)

Branch: master dna / DNA / src / dna / Dna.java

[Find file](#)
[Copy path](#)

leifeld Addressed integer conversion issue in dna\_setDocuments. Fixes #127.

03ba7d9 4 days ago

3 contributors

292 lines (259 sloc) 10.9 KB

[Raw](#)
[Blame](#)
[History](#)

```

1 package dna;
2
3 import dna.dataStructures.*;
4
5 import java.awt.Color;
6 import java.io.PrintStream;
7 import java.util.ArrayList;
8 import java.util.Calendar;
9 import java.util.Date;
10 import java.util.LinkedHashMap;
11
12 import javax.swing.ImageIcon;
13
14 public class Dna {
15     public static Data data = new Data();
16     public static Dna dna;
17     public Gui gui;
18     public SqlConnection sql;
19     public String version, date;
20     PrintStream console;

```

>BBa\_I13600 Part-only sequence (940 bp)

```

tccctatcagtgatagagattgacatccctatcagtgatagagatactgagcactactagagaaaggagagaaatactagatgggtgagcaaggcgagga
gctgttcaccgggggtgggtgcccacctcgtgagctggacggcgagctgaacggccacaagttcagcgtgtccggcgaggcgaggcgatgccacctac
ggcaagctgaccctgaagttcatctgcaccaccggcaagctgcccgtgccctggcccaccctcgtgaccaccctgacctggggcgctgagtgcttcagcc
gctaccccgaccacatgaagcagcacgacttctcaagtcgccatgccgaaggctacgtccaggagcgcaccatcttcttcaaggacgacggcaacta
caagaccgcgccgaggtgaagttcgaggcgacaccctgggtgaaccgcatcgagctgaaggcgcacgttcaaggaggacggcaacatcctggggcac
aagctggagtacaactacatcagccacaacgtctatatcaccgccgacaagcagaagaacggcatcaaggccaacttcaagatccgccacaacatcgagg
acggcagcgtgacgtcgccgaccactaccagcagaacacccccatcgggcgacggccccgtgctgctgcccgaaccactacctgagcaccagtcgcg
cctgagcaaaagacccaacgagaagcgcatcacatggctcgtgagttcgtgaccgccggggatcactctcgcatggacgagctgtacaagtaa
taatactagagccaggcatcaataaaacgaaaggctcagtcgaaagactgggcctttcgtttatctgtgtttgtcgggtgaacgctctctactagat
cacactggctcaccttcgggtgggcctttctgcgtttata

```

# OPEN SOURCE PARALLELS

## Tet with CFP reporter (without LVA tag)

The part glows (rather weakly) with a cyan colored fluorescent protein. The part is constitutive. tetR represses CFP production; this repression can be overcome by adding tetracycline.

Sequence and Features

[Subparts](#)
[Ruler](#)
[SS](#)
[DS](#)
 Length: 940 bp

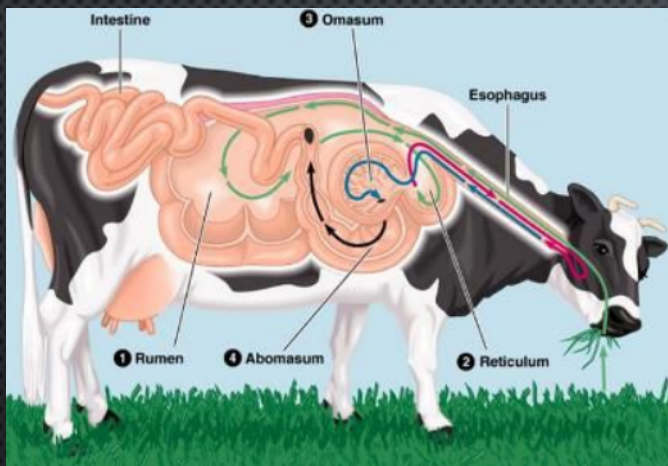


parts.igem.org/Part:BBa\_I13600 24

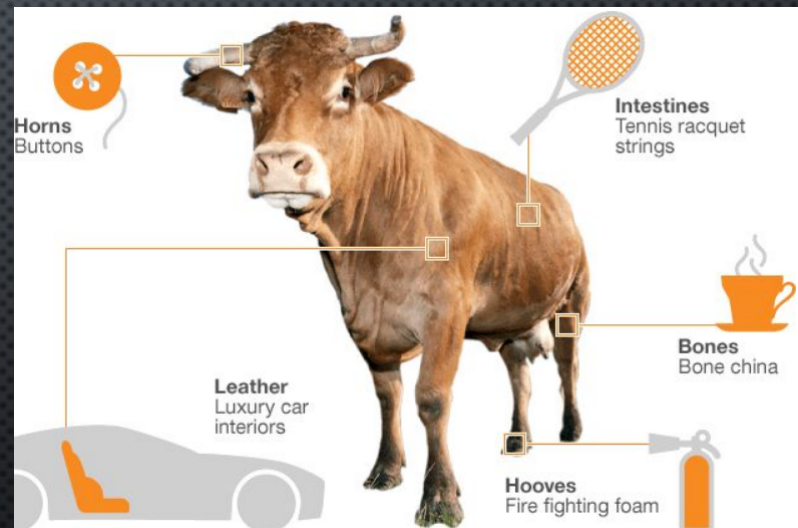
github.com/leifeld/dna/blob/master/DNA/src/dna/Dna.java



# AFTER TEN WEEKS OF LAB WORK



A plan to reduce methane emissions from cattle by altering digestion biome using engineered *E. coli*



<http://2017.igem.org/Team:UNebraska-Lincoln/Description>

# SB SAFETY CONCERNS

“FDA IS AWARE THAT GENE THERAPY PRODUCTS INTENDED FOR SELF-ADMINISTRATION AND 'DO IT YOURSELF' KITS TO PRODUCE THERAPIES FOR SELF-ADMINISTRATION ARE BEING MADE AVAILABLE TO THE PUBLIC. **THE SALE** OF THESE PRODUCTS IS AGAINST THE LAW. FDA IS CONCERNED ABOUT THE SAFETY RISKS INVOLVED.” [1]

**MAYBE BIOHACKERS SHOULD MAKE ASSURANCE CASES FOR THEIR DESIGNS?**

[1] [www.fda.gov/BiologicsBloodVaccines/CellularGeneTherapyProducts/ucm586343.htm](http://www.fda.gov/BiologicsBloodVaccines/CellularGeneTherapyProducts/ucm586343.htm)

[2] [www.livescience.com/62449-aaron-traywick-death.html](http://www.livescience.com/62449-aaron-traywick-death.html)

## 'Biohacker' Who Injected Himself with DIY Herpes Treatment Found Dead

By Sara G. Miller, Health Editor | May 1, 2018 12:25pm ET



MORE ▾

Health without the hype:  
Subscribe now to stay in the know.

Subscribe to  
LiveScience ›



Credit: Ford Fischer/News2Share

The CEO of a biomedical startup who sparked controversy when he injected himself with an untested [herpes](#) treatment in front of a live audience in February has died, according to an email sent to Live Science.

[2]



# ASSURANCE CASES FOR MEDICAL DEVICES

## U.S. FOOD AND DRUG ADMINISTRATION (FDA) INSULIN PUMP INITIATIVE [1]

[1]

[www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202511.htm](http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202511.htm)

**threatpost** CATEGORIES FEATURED PODCASTS VIDEOS

Join thousands of people who receive the latest breaking **cybersecurity news** every day.

Welcome > Blog Home > Vulnerabilities > Vulnerabilities in Insulin Pumps Can Lead to Overdose



**VULNERABILITIES IN INSULIN PUMPS CAN LEAD TO OVERDOSE**

by **Chris Brook** October 4, 2016, 1:16 pm

Patients who use insulin pumps made by Johnson & Johnson are being warned this week that vulnerabilities in the devices could be exploited to trigger an overdose.

The bugs exist in OneTouch Ping, a medical device made by Animas Corp. – a subsidiary of Johnson & Johnson – which allows diabetic patients to self-administer insulin.

[threatpost.com/vulnerabilities-in-insulin-pumps-can-lead-to-overdose/121064/](http://threatpost.com/vulnerabilities-in-insulin-pumps-can-lead-to-overdose/121064/) 27

# ASSURANCE CASES FOR SEBOs

- IN PRIOR WORK, WE INVESTIGATED USING ASSURANCE CASES TO ADDRESS **DYNAMIC** QUALITIES OF SEBOs AS SAFETY-CRITICAL SYSTEMS [1]
  - EVOLUTION
  - MUTATION
- WE NOW PRESENT A NEW ABSTRACTION, A TEMPLATE-LIKE MODEL WE CALL AN **ASSURANCE RECIPE**



Uranium glass

[1] Cohen, Myra B., Justin Firestone, and Massimiliano Pierobon. "The Assurance Timeline: Building Assurance Cases for Synthetic Biology." In *International Conference on Computer Safety, Reliability, and Security*, pp. 75-86. Springer, Cham, 2016.

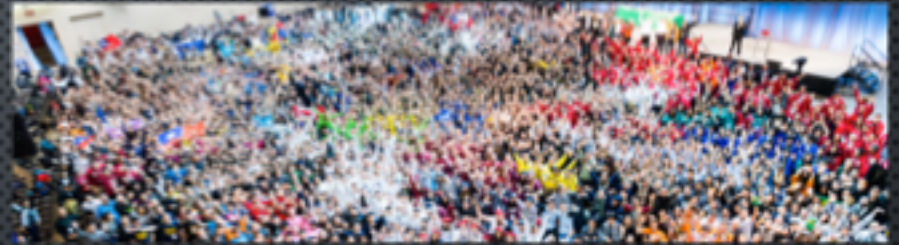


# OUR CONTRIBUTIONS

- FIRST: THE CONCEPT OF THE ASSURANCE RECIPE
- SECOND: EXAMPLE RECIPES FOR SB USING THE CLAIM FORMALIZATION PATTERN OF DENNEY AND PAI
  - A SAFETY-MECHANISM RECIPE WITH THREE EXAMPLE INSTANTIATIONS
  - A CONTAINMENT RECIPE WITH ONE EXAMPLE INSTANTIATION

# PRE-STUDY: THE iGEM COMPETITION

- WE MANUALLY EXAMINED THREE YEARS OF GOLD-MEDAL PROJECTS (2015-2017)
- GOLD-MEDAL TEAMS MUST “CONSIDER WHETHER THEIR PROJECTS ARE SAFE, RESPONSIBLE, AND GOOD FOR THE WORLD”
- OUR GOAL: BUILD ASSURANCE RECIPES AND INSTANTIATE THEM USING THE MOST COMMON SAFETY FEATURES FROM GOLD-MEDAL TEAMS



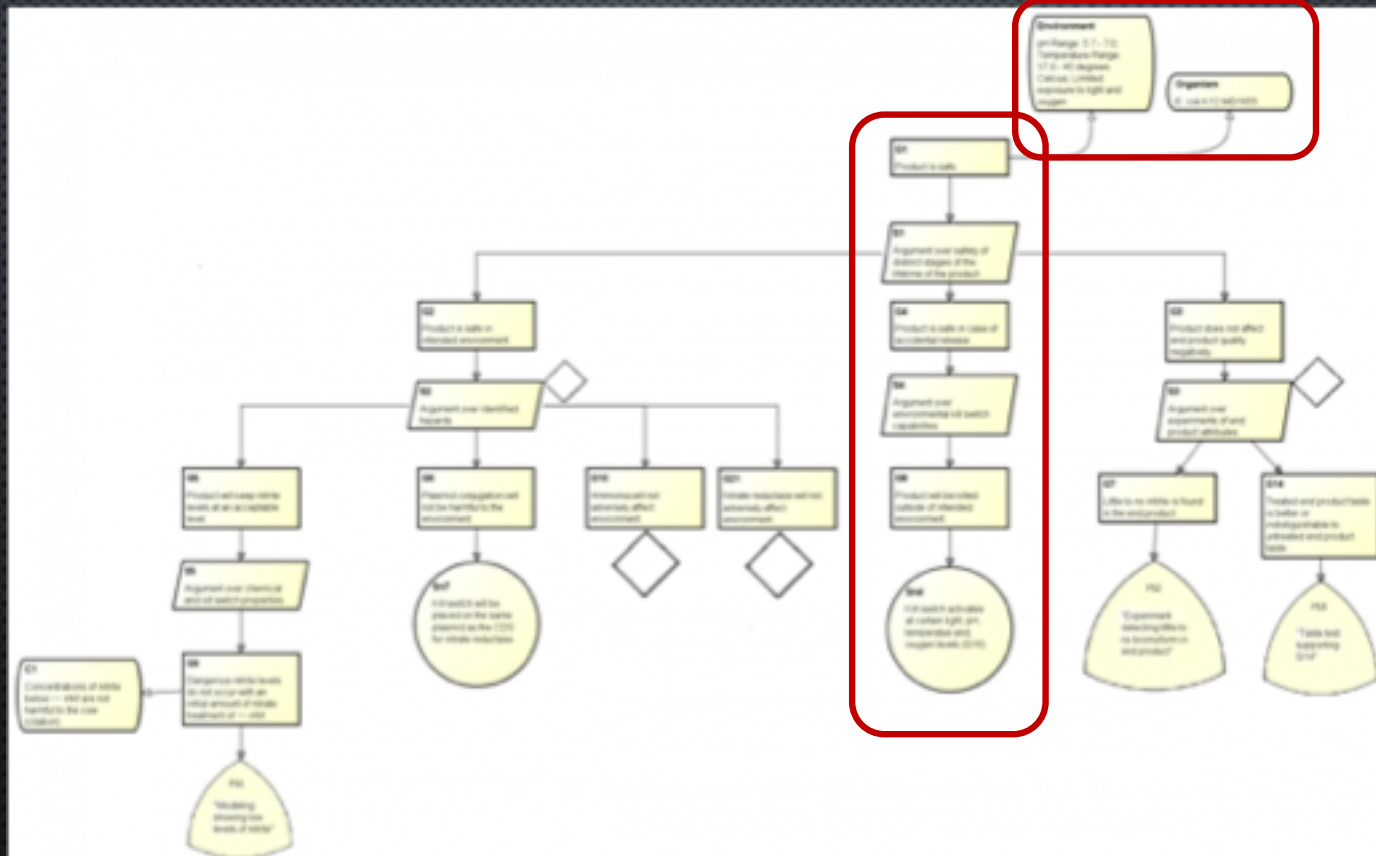
[http://2017.igem.org/wiki/images/f/ff/HQ\\_About2017\\_1.png](http://2017.igem.org/wiki/images/f/ff/HQ_About2017_1.png)



## PRE-STUDY: THE iGEM COMPETITION

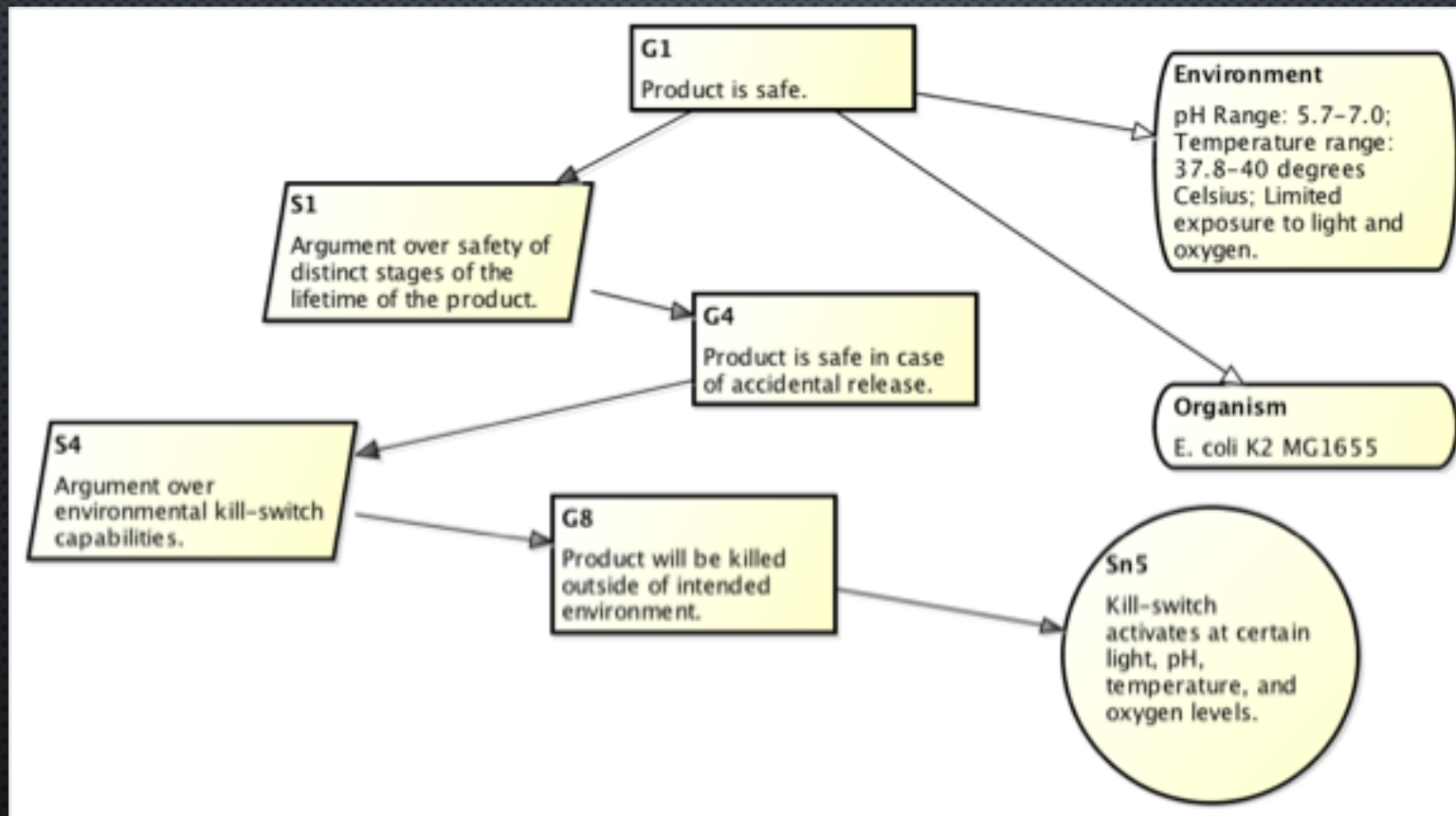
Year	Gold Medals	GRAS	Containment	Kill-switch	Auxotrophy	Degradation
2015	114	50.00%	14.04%	7.02%	3.51%	1.75%
2016	111	43.24%	20.72%	12.61%	2.70%	5.41%
2017	109	44.04%	16.51%	13.76%	6.42%	6.42%

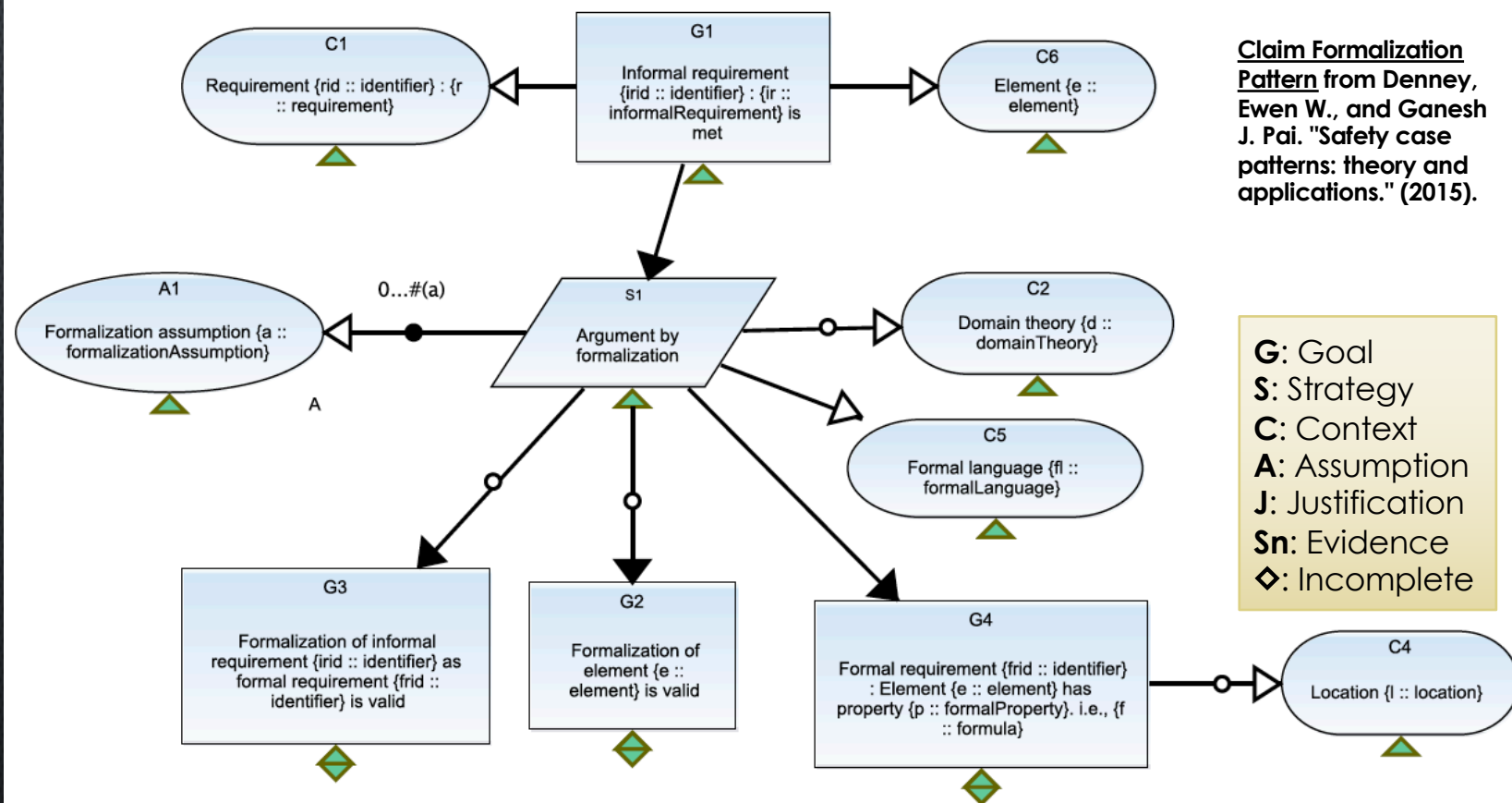
# ASSURANCE CASE FOR SEBO KILL-SWITCH (UNL 2017)





# EXAMPLE FOR A KILL-SWITCH







# DIFFICULTIES FOR EVEN SB EXPERTS?

- IT SEEMED FAIRLY CLEAR THAT IGEM TEAMS (UNDERGRADUATES) STRUGGLED WITH CREATING AN ASSURANCE CASE
- EVEN AN SB EXPERT IS LIKELY TO STRUGGLE BUILDING AN ASSURANCE CASE GIVEN A PATTERN



PATTERN

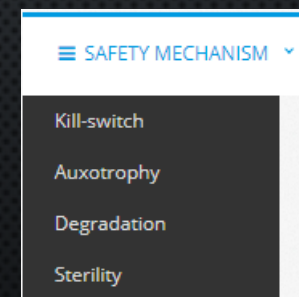
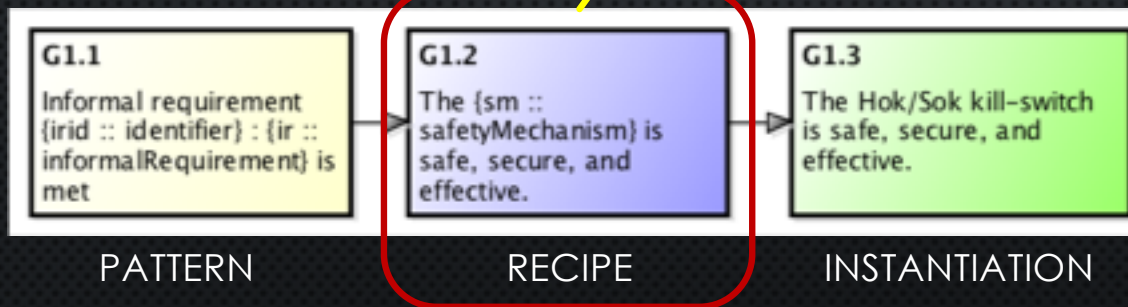
INSTANTIATION



# THE “ASSURANCE RECIPE”

- INTUITION: SYNTHETIC BIOLOGISTS ARE NOT EXPERTS IN SOFTWARE ENGINEERING OR ASSURANCE CASES
- COMMON PROBLEMS HAVE COMMON SOLUTIONS
- FORMAL PATTERNS ARE TOO HIGH LEVEL FOR MOST USERS

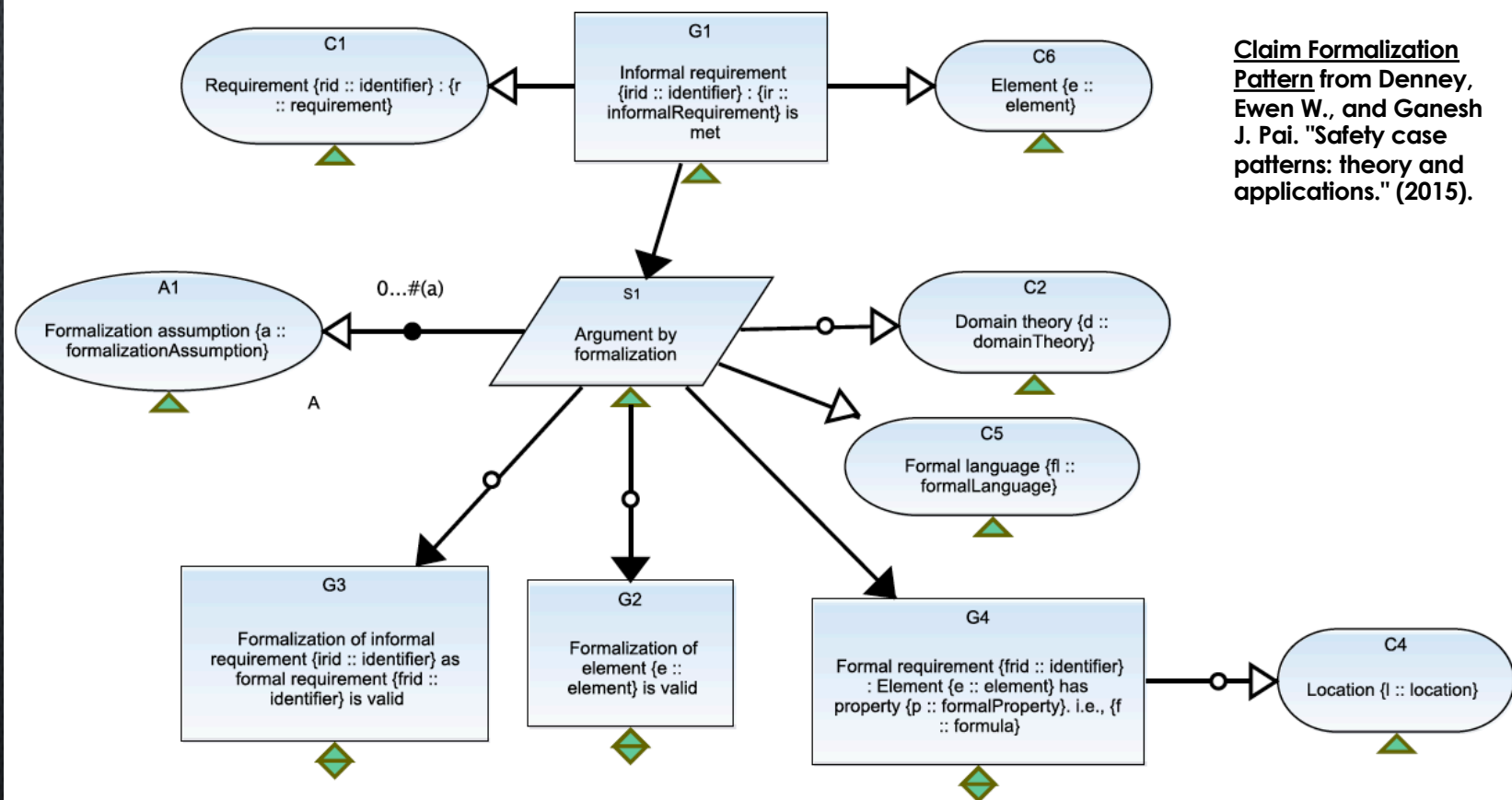
Variable	Ingredients
sm :: safetyMechanism	1. Kill-switch
	2. Auxotrophy
	3. Degradation
	4. Sterility
u :: usage	1. The SEBOs
	2. Only the SEBOs' outputs
se :: specificEnvironment	1. Soil
	2. Water table
	3. [Specific species habitat]
	4. Atmosphere
	5. Rivers
	6. Freshwater rivers or lakes
	7. Saltwater lakes or oceans
	8. Human body
	9. [Non-human] body
sp :: specificParameter	1. [Temperature Range]
	2. [pH Range]
	3. [Aerobic/Anaerobic] environment
	5. [Natural/Specific frequencies/Absence] of light
	7. [Presence/Absence] of nutrients
	8. [Altitude range]





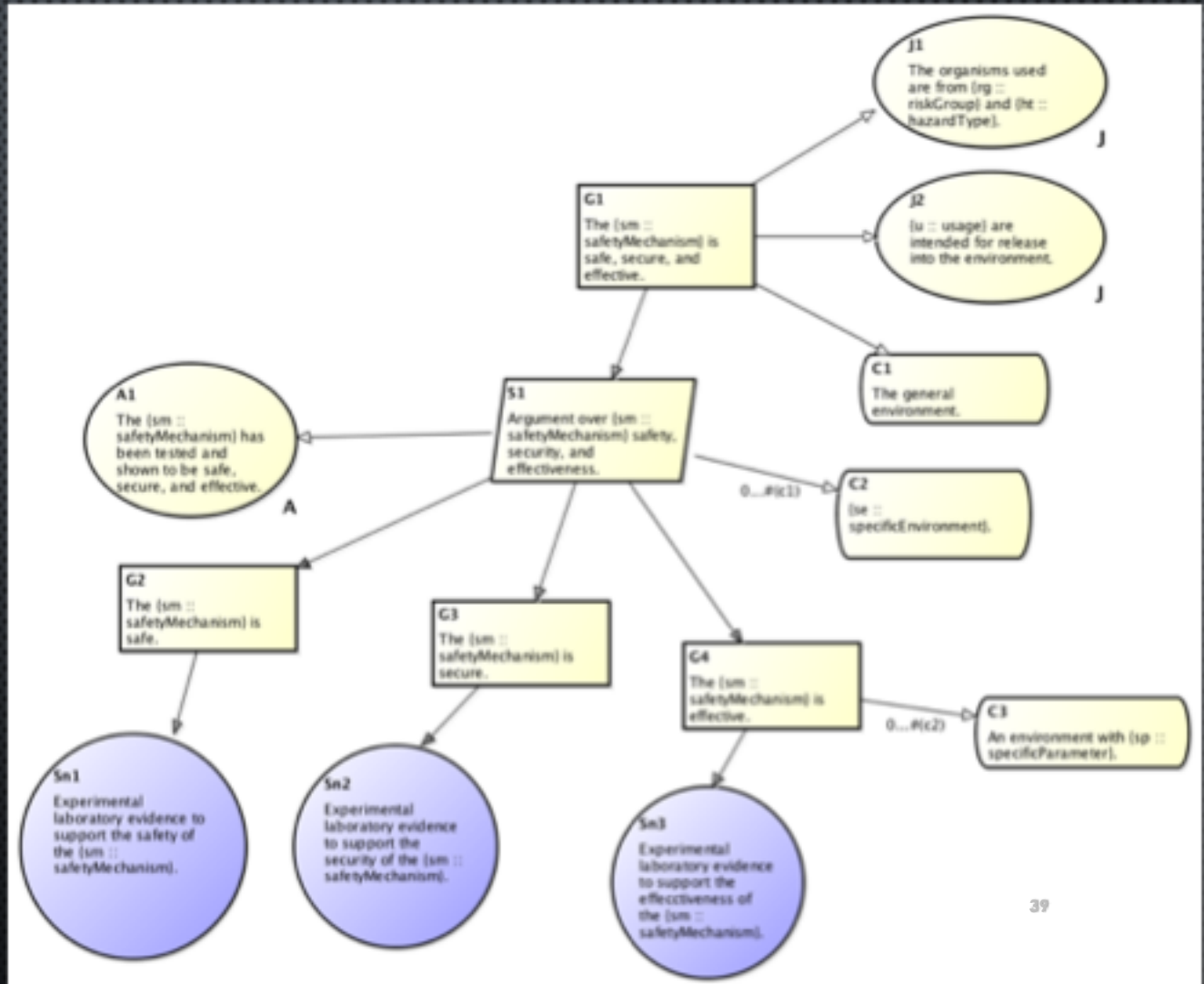
# PRESENTATION OUTLINE

- MOTIVATION
- BACKGROUND ON SYNTHETIC BIOLOGY
- PRE-STUDY
- THE ASSURANCE RECIPE
- FEASIBILITY STUDY
- CONCLUSION





# RECIPE 1: A SAFETY MECHANISM RECIPE

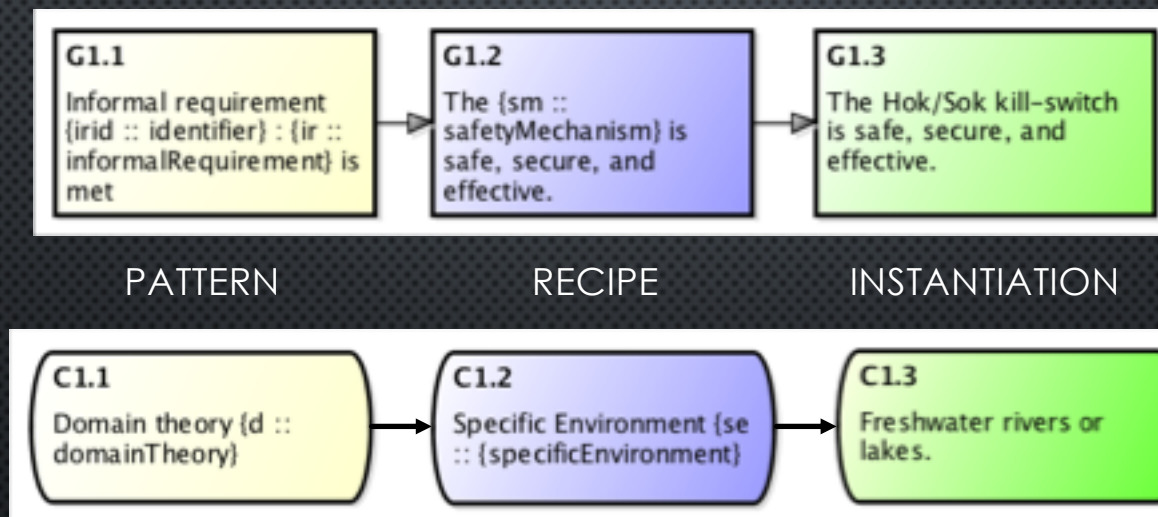


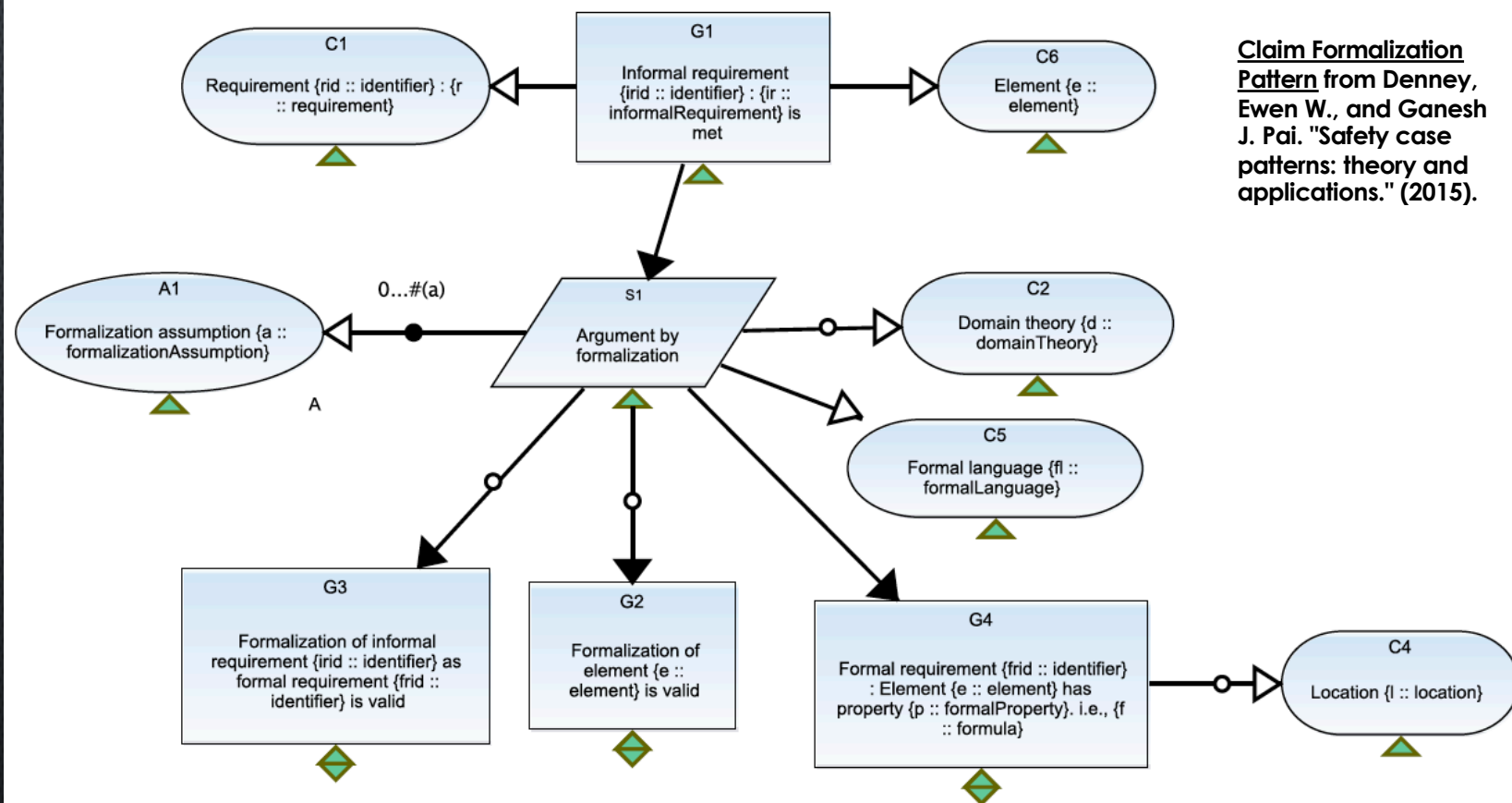
# INSTANTIATE THE SAFETY MECHANISM RECIPE FOR A KILL-SWITCH





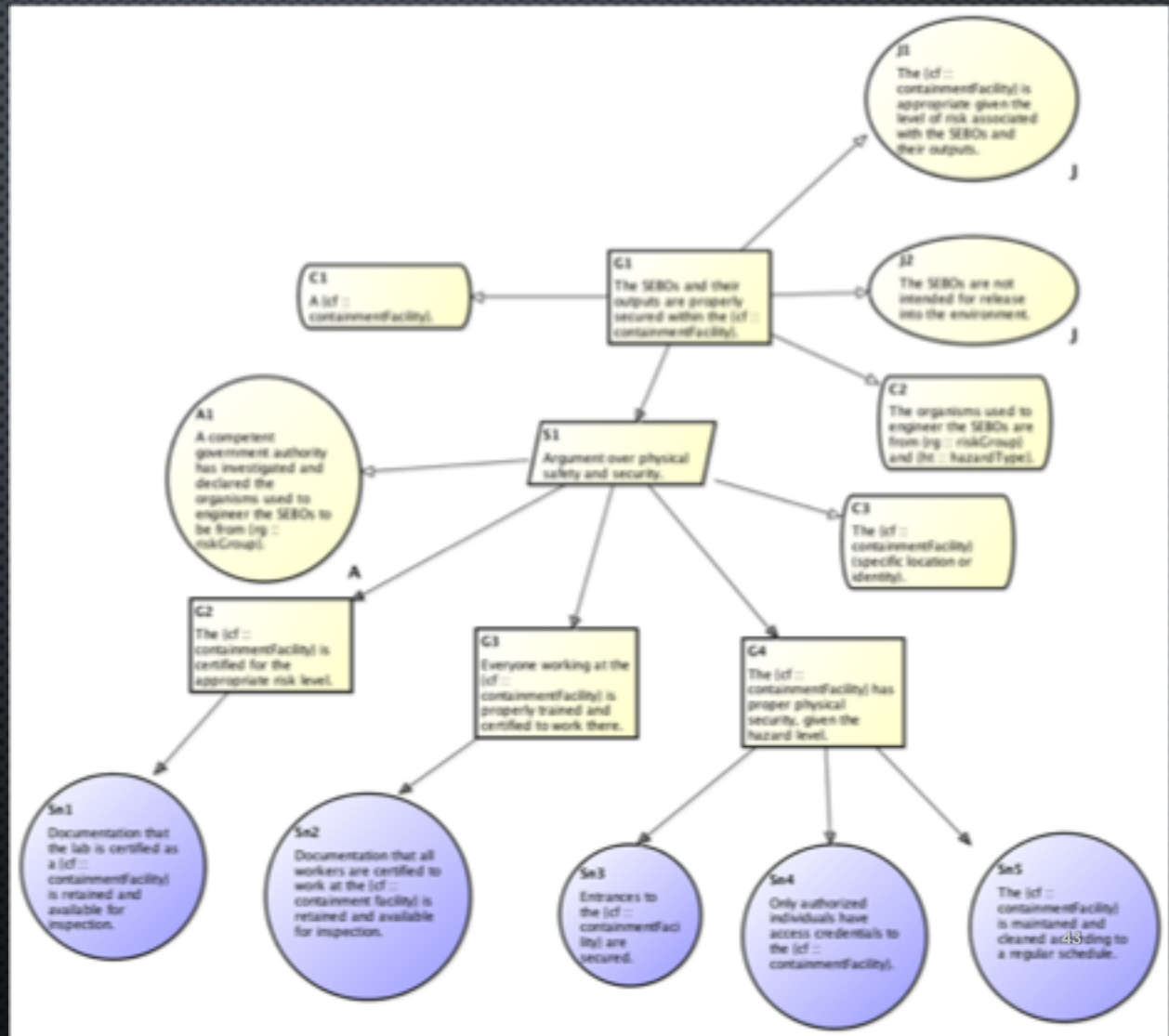
# FROM PATTERN TO RECIPE TO INSTANTIATION



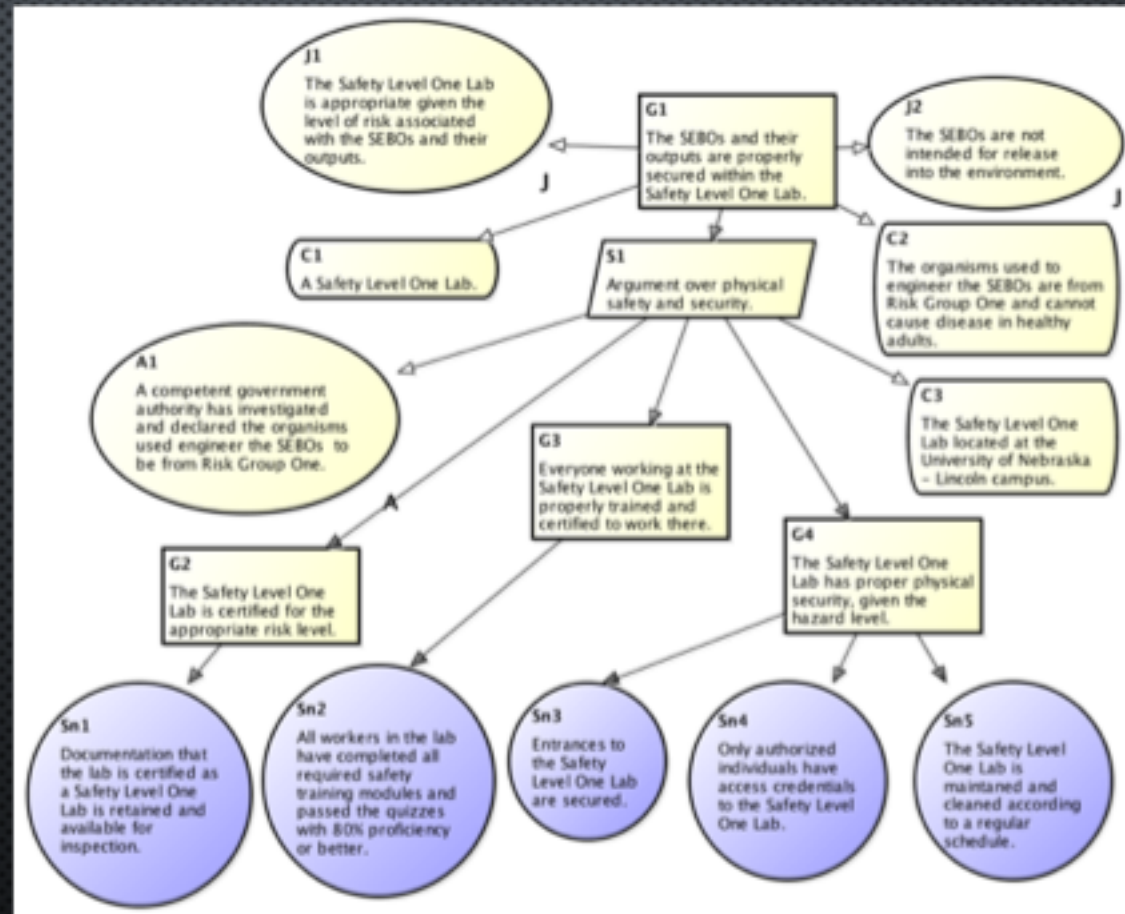




## RECIPE 2: A CONTAINMENT RECIPE

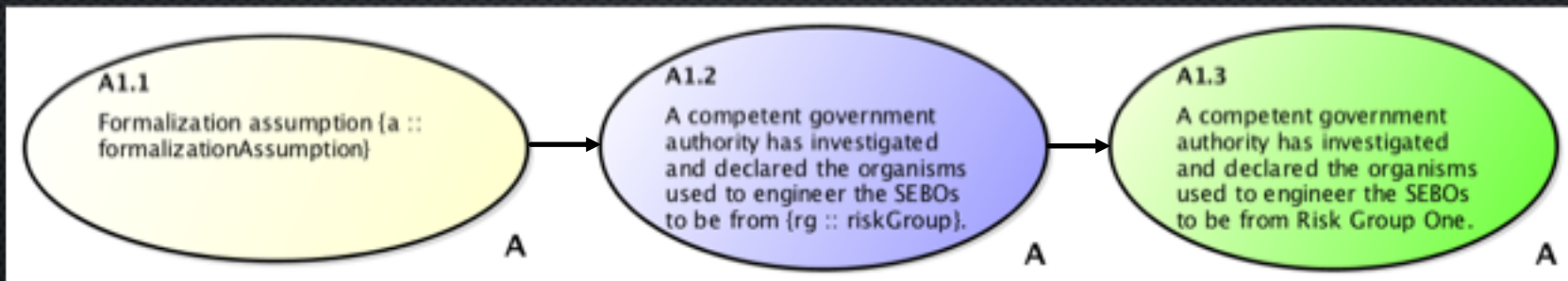
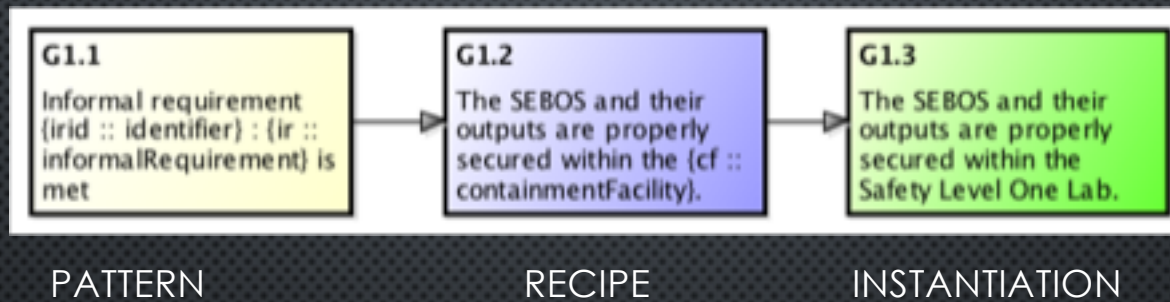


# INSTANTIATE THE CONTAINMENT RECIPE FOR A SAFETY-LEVEL ONE LAB





# FROM PATTERN TO RECIPE TO INSTANTIATION



## FUTURE WORK: INTERACTIVE RECIPES ONLINE

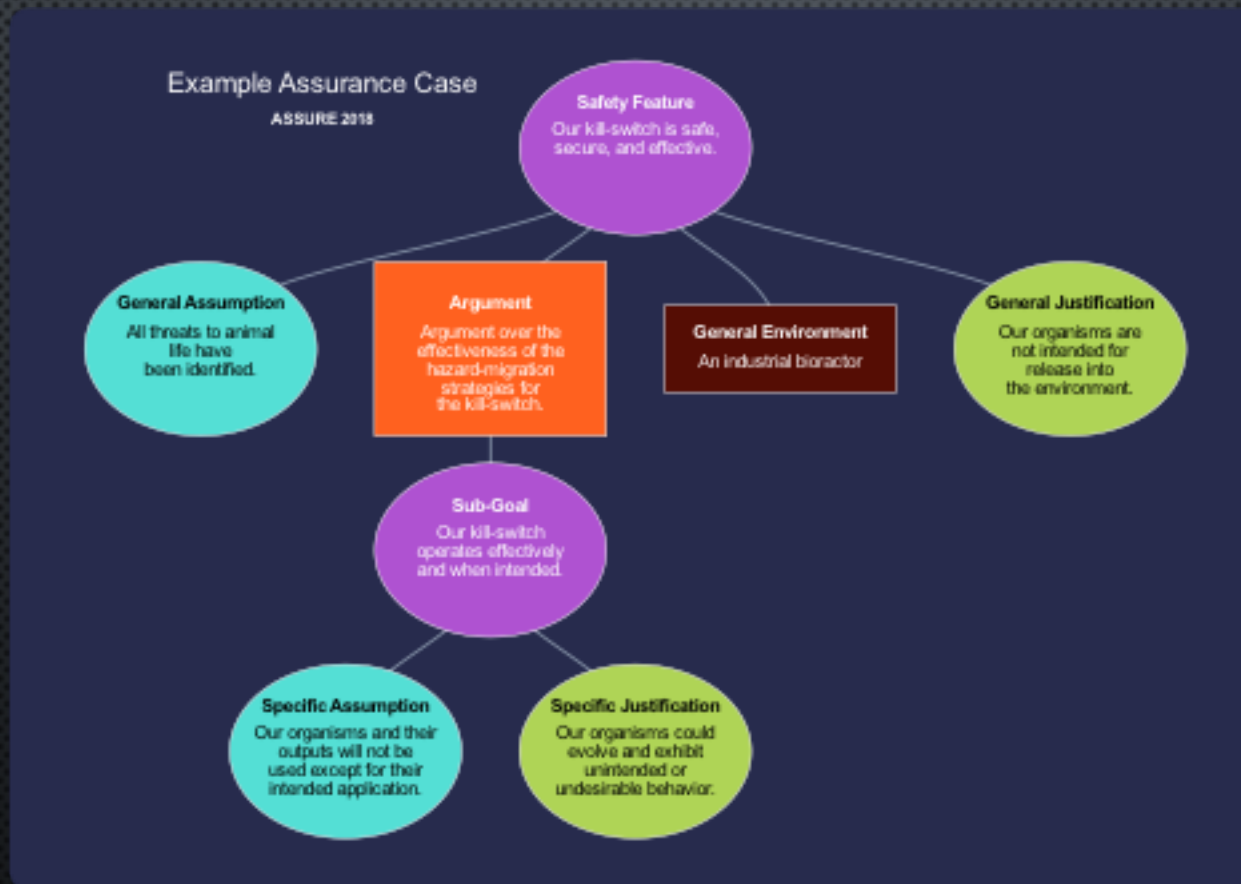
- ASK NOVICE USERS TO USE RECIPES TO BUILD THEIR OWN ASSURANCE CASES
- FORMALIZE A PROCESS TO GENERALIZE RECIPES FOR OTHER DISCIPLINES
- THE 2018 UNL iGEM TEAM IS WORKING ON A WEBSITE FOR OTHER iGEM TEAMS (COMPETITION TO BE HELD OCTOBER 24-28, 2018) BASED ON OUR RECIPES AND INGREDIENTS



# FUTURE WORK: INTERACTIVE RECIPES ONLINE

Title	<input type="text"/>
Description	<input type="text"/>
Safety Feature	<div>Kill-Switch ▼</div>
General Assumption	<div>All threats to the environment have been identified. ▼</div>
General Environment	<div>Only in the lab ▼</div>
General Justification	<div>Our organisms only function in fresh water. ▼</div>
Goal	<div>Our kill-switch operates effectively and when intended. ▼</div>
Specific Assumption	<div>Our lab has adequate physical security. ▼</div>
Specific Justification	<div>Our organisms could evolve and exhibit unintended or undesirable behavior. ▼</div>
<div>Save</div>	

# FUTURE WORK: INTERACTIVE RECIPES ONLINE



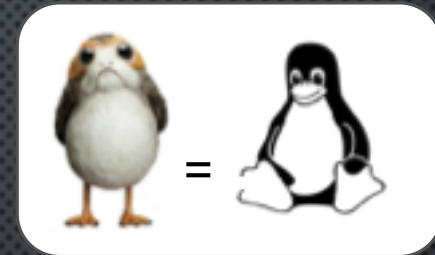


# A COLLABORATIVE SOLUTION

- REGULATORY AGENCIES, INDUSTRY, AND RESEARCHERS WORK TOGETHER TO ITERATIVELY IMPROVE RECIPES AND SUGGESTED INGREDIENTS
- SUGGESTION: AGENCIES SHOULD REQUIRE ASSURANCE CASES TO SHOW RISK ANALYSIS AND RISK MITIGATION



# CONCLUSION



- ASSURANCE RECIPES CAN HELP ENGINEERS FROM OTHER SAFETY-CRITICAL DISCIPLINES CONSIDER SAFETY EARLIER IN THE DESIGN PROCESS AND ASSIST REGULATORY AGENCIES WITH CERTIFICATION
- WE HAVE DEMONSTRATED THE APPLICATION OF ASSURANCE RECIPES AND ASSURANCE CASES TO THE EMERGING DISCIPLINE OF SB