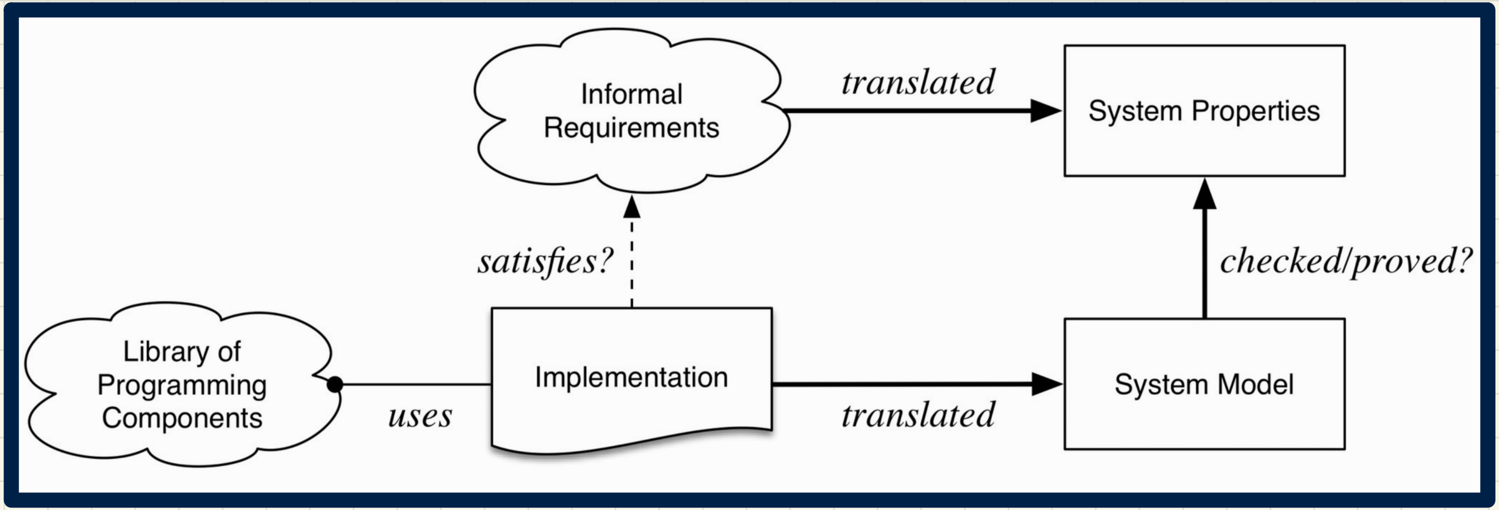
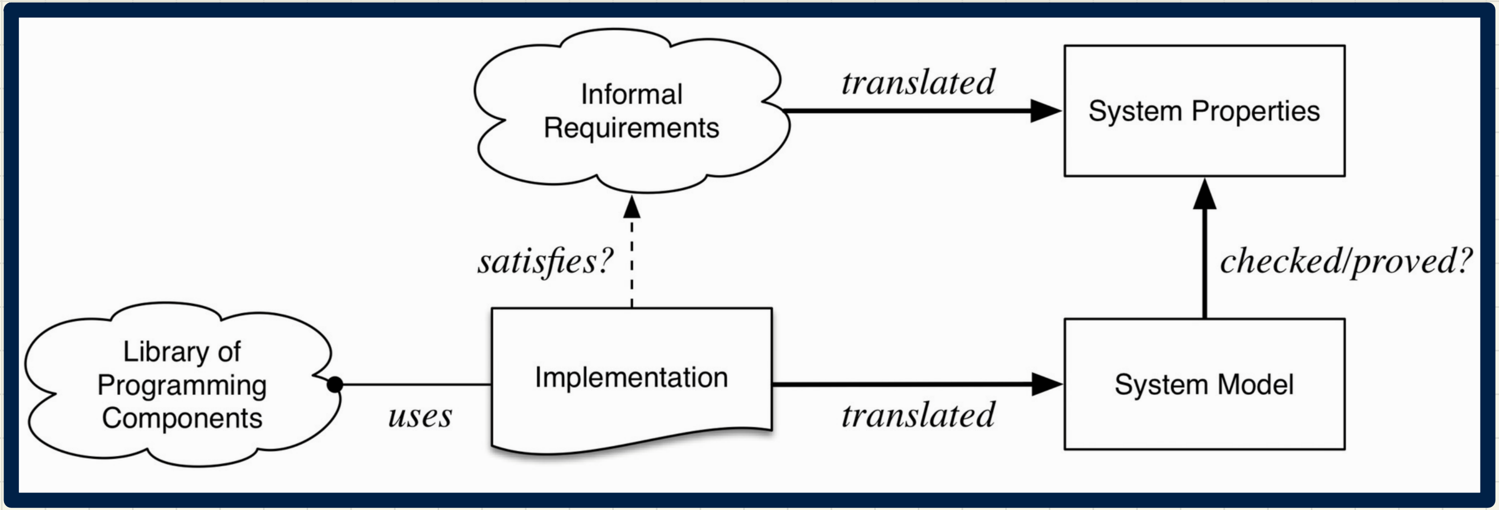
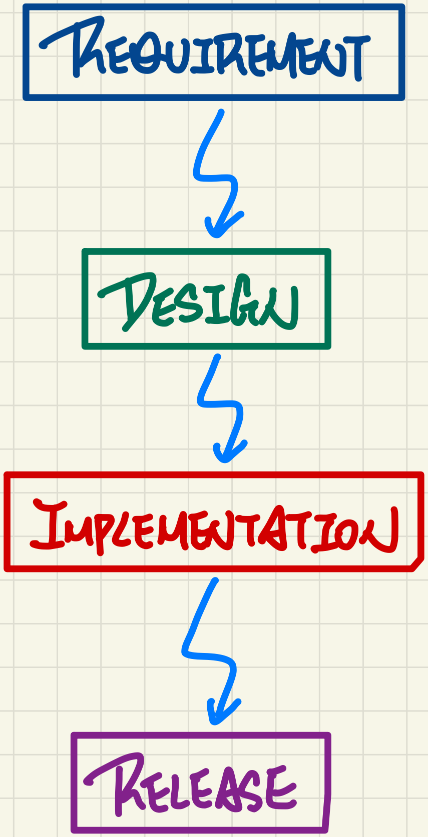
Building the product right?



Building the right product?



Software Development Process



- Natural Language
  (incomplete, ambiguous, contradicting)
- Requirement Elicitation

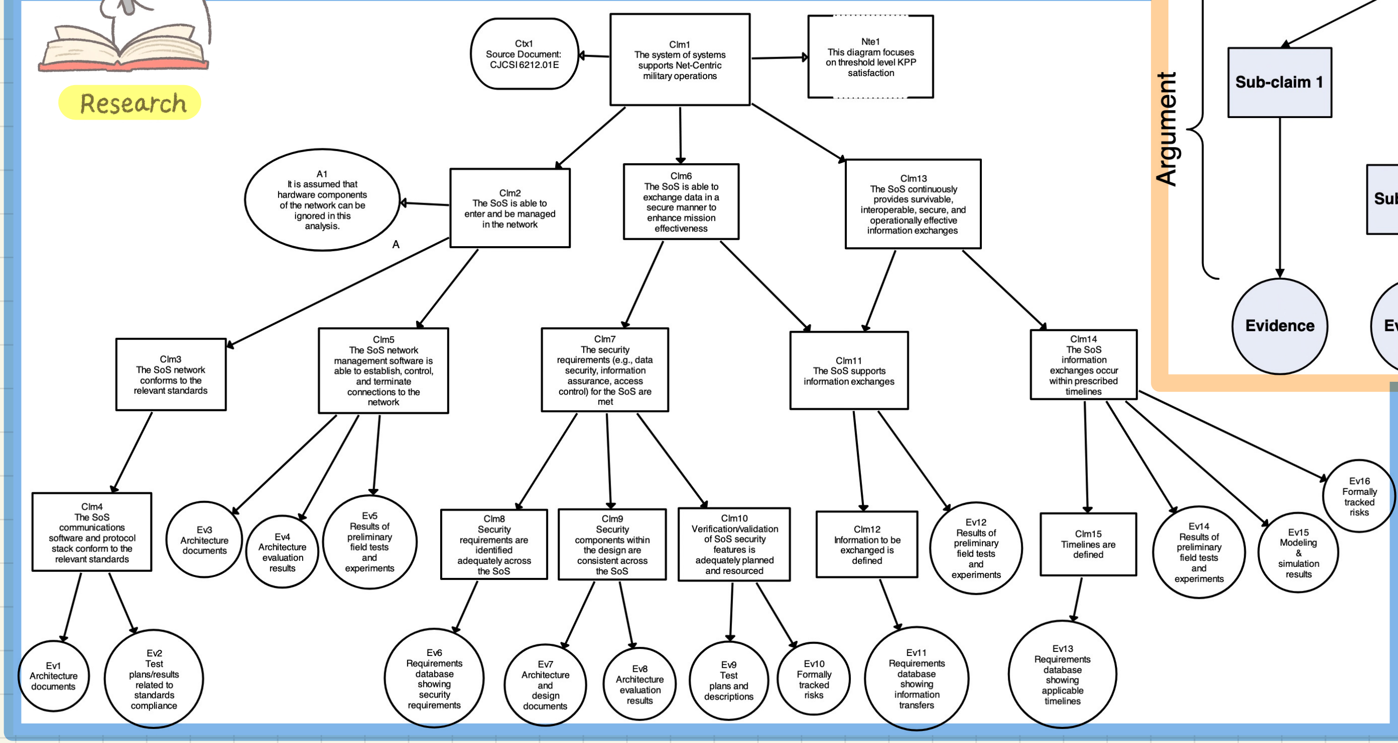
- Blueprints
- Not necessarily executable & testable

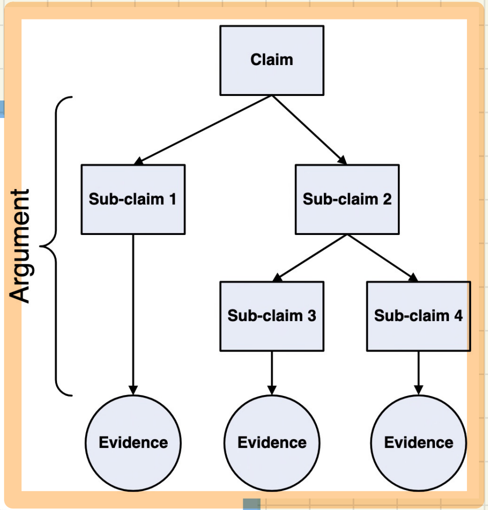
- API Given
- Efficient (data structures & algorithms)
- Unit Tests

- Customer's Acceptance
- Recall?

Certifying Systems: Assurance Cases

Research on "Assurance Cases" if interested!

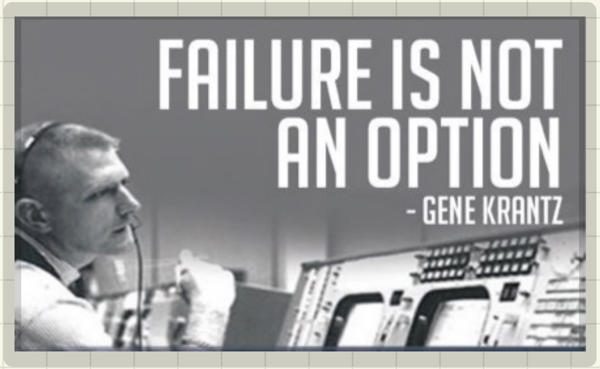

Ctx1
Source Document: CJCSI 6212.01E
Clm1
The system of systems supports Net-Centric military operations
Nte1
This diagram focuses on threshold level KPP satisfaction
A1
It is assumed that hardware components of the network can be ignored in this analysis.
A
Clm2
The SoS is able to enter and be managed in the network
Clm6
The SoS is able to exchange data in a secure manner to enhance mission effectiveness
Clm13
The SoS continuously provides survivable, interoperable, secure, and operationally effective information exchanges
Clm3
The SoS network conforms to the relevant standards
Clm5
The SoS network management software is able to establish, control, and terminate connections to the network
Clm7
The security requirements (e.g., data security, information assurance, access control) for the SoS are met
Clm11
The SoS supports information exchanges
Clm14
The SoS information exchanges occur within prescribed timelines
Ev16
Formally tracked risks
Clm4
The SoS communications software and protocol stack conform to the relevant standards
Ev3
Architecture documents
Ev4
Architecture evaluation results
Ev5
Results of preliminary field tests and experiments
Clm8
Security requirements are identified adequately across the SoS
Clm9
Security components within the design are consistent across the SoS
Clm10
Verification/validation of SoS security features is adequately planned and resourced
Clm12
Information to be exchanged is defined
Ev12
Results of preliminary field tests and experiments
Clm15
Timelines are defined
Ev14
Results of preliminary field tests and experiments
Ev15
Modeling & simulation results
Ev1
Architecture documents
Ev2
Test plans/results related to standards compliance
Ev6
Requirements database showing security requirements
Ev7
Architecture and design documents
Ev8
Architecture evaluation results
Ev9
Test plans and descriptions
Ev10
Formally tracked risks
Ev11
Requirements database showing information transfers
Ev13
Requirements database showing applicable timelines



Source: https://resources.sei.cmu.edu/asset_files/whitepaper/2009_019_001_29066.pdf

Correct by Construction

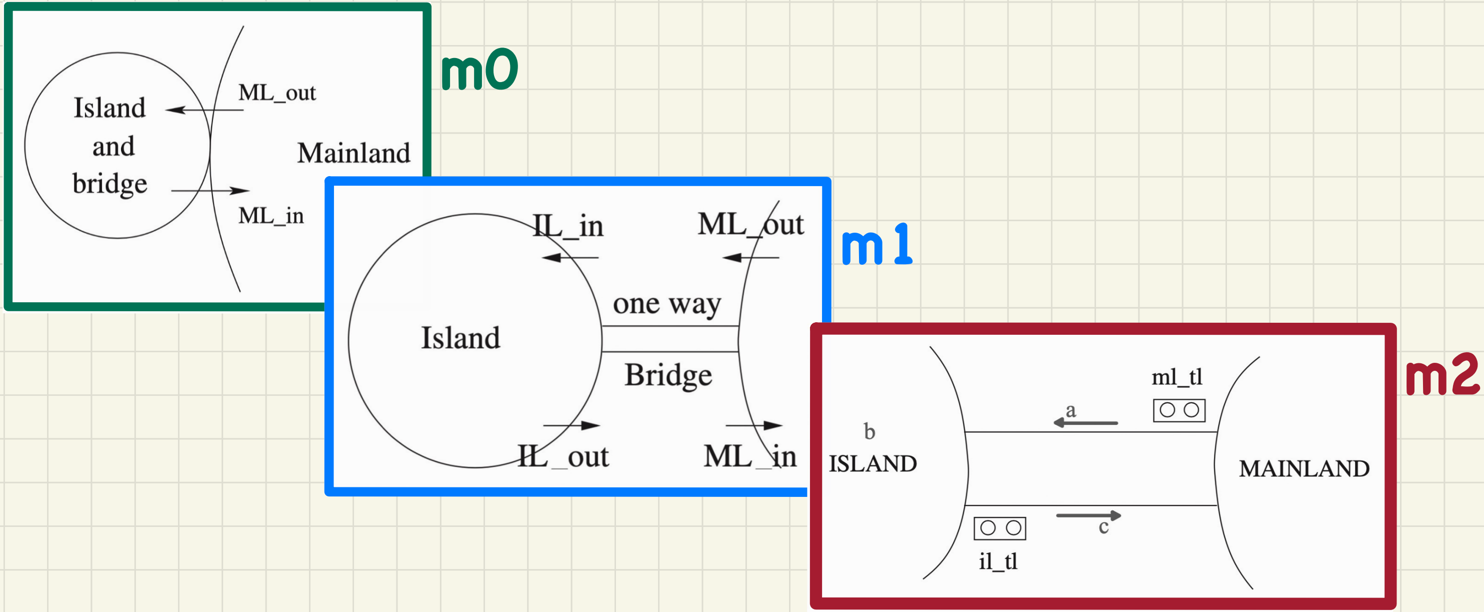
$$\begin{tikzcd} \boxed{m_0} \arrow[r] & \cdots \arrow[r] & \boxed{m_i} \arrow[r] & \boxed{m_j} \arrow[r] & \cdots \arrow[r] & \boxed{m_n} \end{tikzcd}$$



Source: https://audiobookstore.com/audiobooks/failure-is-not-an-option-1.aspx

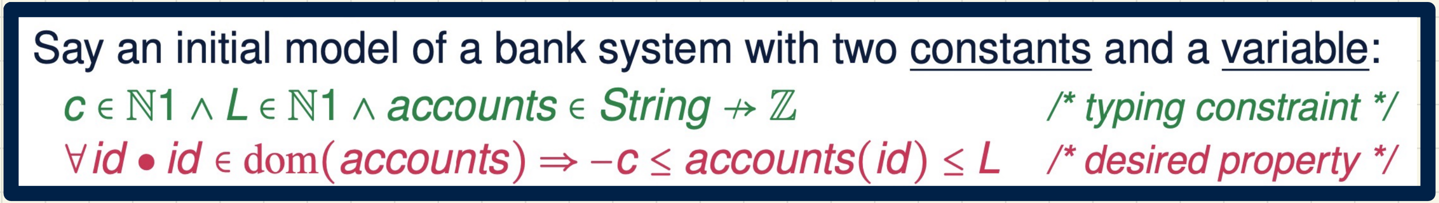
Correct by Construction: Bridge Controller System

$$m_0 \to \cdots \to m_i \to m_j \to \cdots \to m_n$$



State Space of a Model

Definition: The state space of a model is the set of **all** possible valuations of its declared constants and variables, subject to declared constraints.



Say an initial model of a bank system with two constants and a variable:

$c \in \mathbb{N}1 \land L \in \mathbb{N}1 \land accounts \in String \mathrel{+\!\!\!\!\rightarrow} \mathbb{Z}$ /* typing constraint */

$\forall id \bullet id \in \mathrm{dom}(accounts) \Rightarrow -c \le accounts(id) \le L$ /* desired property */

Q1. Give some example configurations of this initial model's state space.

Q2. How large exactly is this initial model's state space?

Exercise: Theorem Proving vs. Model Checking

Variable:

An integer counter c

Safety Constraints:

MIN_VALUE <= c <= MAX_VALUE

Unconditional Update:

init: initializes c as zero

Conditional Updates:

inc: increments c when ??

dec: decrements c when ??