Requirements, Validation and Risk

Answer · Recommended for you

Why should I hire a software engineer if I can just copy and paste code from Stack Overflow?

The Story So Far …

- We want to build a quality product
- What are we supposed to be building, again?
- We should ask the customer!
  - But how?

One-Slide Summary

- **Requirements elicitation** relies on communication with **stakeholders**. This includes identifying relevant parties, understanding the domain, interviews, and the exploration of alternatives. Requirements often conflict.
- **Validation** checks the correctness of requirements; **verification** checks the correctness of software.
- **Risk** includes both the likelihood and the consequence of failure.

Requirements Elicitation

- **Requirements elicitation** is the process of identifying system requirements through communication with stakeholders. Typically:

  Step 1. Identify stakeholders

  Step 2. Understand the domain

  - Analyze artifacts, interact with stakeholders

  Step 3. Discover the real needs

  - Interview stakeholders, resolve conflicts

  Step 4. Explore alternatives to address needs

Stakeholder

- A **stakeholder** is any person or group who will be affected by the system, directly or indirectly
  - Customers, other parts of your own organization, regulatory bodies, etc.
- Stakeholders may disagree
- Requirements process should trigger negotiation to resolve conflicts
- (We will return to conflicts later)

"Again this year, you get one wish... but please don't waste it on something even I can't grant, like clear business requirements."

Stakeholder Analysis

- Common criteria for identifying relevant stakeholders include:
- Relevant positions in the organization
- Effective role in making decisions about the system
- Level of domain expertise
- Exposure to perceived problems
- Influence in system acceptance
- Personal objectives and conflicts of interest

NASA Example of Stakeholders

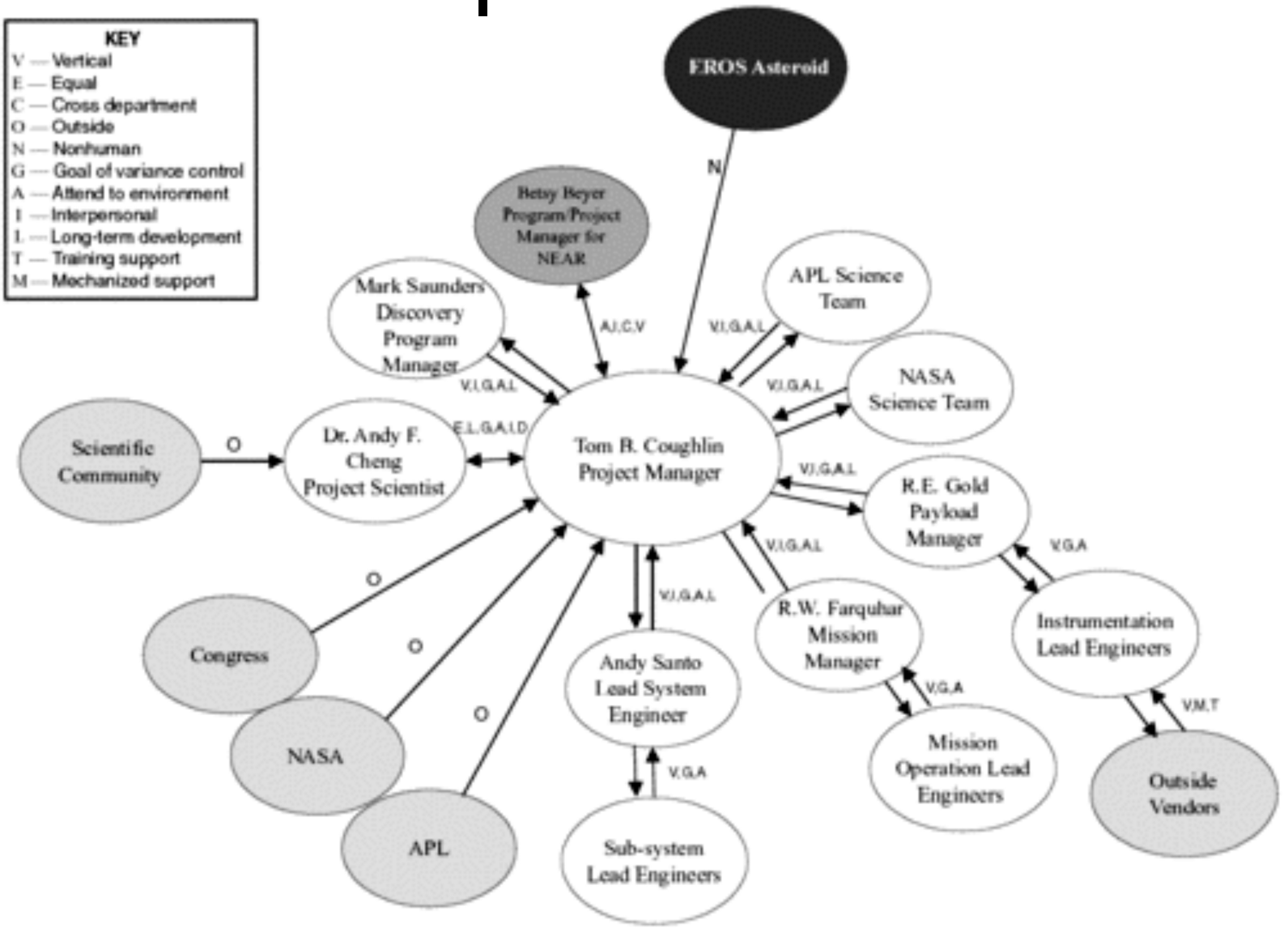


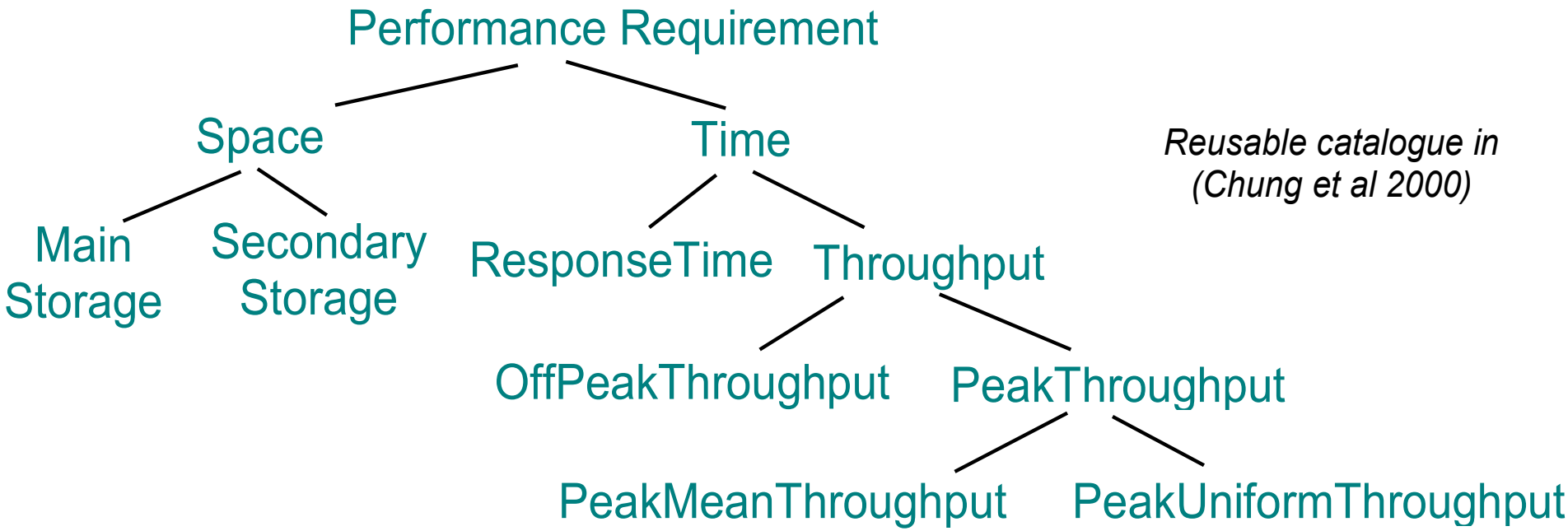
FIGURE 6-3 Role network for National Aeronautics and Space Administration (NASA's) Near Earth Asteroid Rendezvous project.

Step 2: Understanding the Domain

- **Content analysis** involves learning about the system domain
  - Books, articles, wikipedia, etc.
- This often focuses on the system to be built or replaced
  - How does it work? What are the problems? Are there manuals? Bug reports?
- But it also involves the organization
- And reusing knowledge from other systems

Domain-Independent Checklist

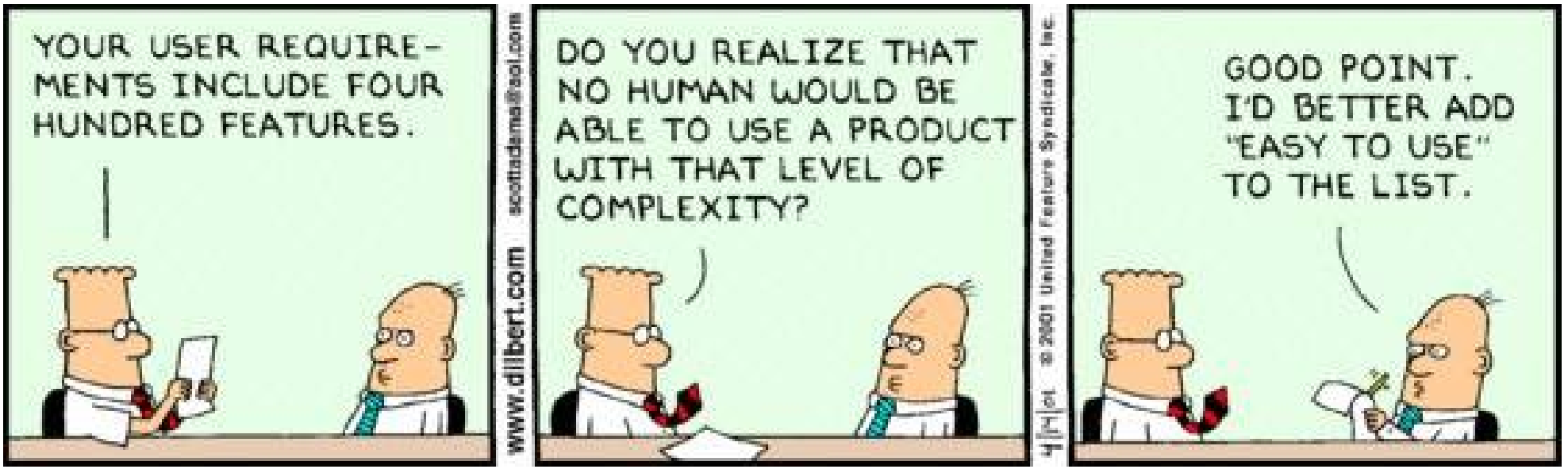
- Consider the list of qualities (from the previous lecture) and select relevant ones
  - Privacy, security, reliability, etc.
  - Even “performance” can be complicated:



Reusable catalogue in (Chung et al 2000)

Step 3:
Discover Real Needs via Interviews

- Having identified stakeholders of interest and information to be gathered …
- Conduct an **interview**



Step 3:
Discover Real Needs via Interviews

- Having identified stakeholders of interest and information to be gathered …
- Conduct an **interview**
  - This can be structured or unstructured, individual or group, etc.
  - It may even be a simple phone call or telecon
- Record and transcribe interview
- Report important finding
- Check validity of report with interviewee

Requirements Interview Advice

- Get basic facts about the interviewee before (role, responsibilities, …)
- Review interview questions before interview
- Begin concretely with specific questions, proposals: work through prototype or scenario
- Be open-minded; explore additional issues that arise naturally, but stay focused on the system
- Contrast with current system or alternatives
  - Explore conflicts and priorities
- Plan for follow-up questions

Example: Identifying Problems (1)

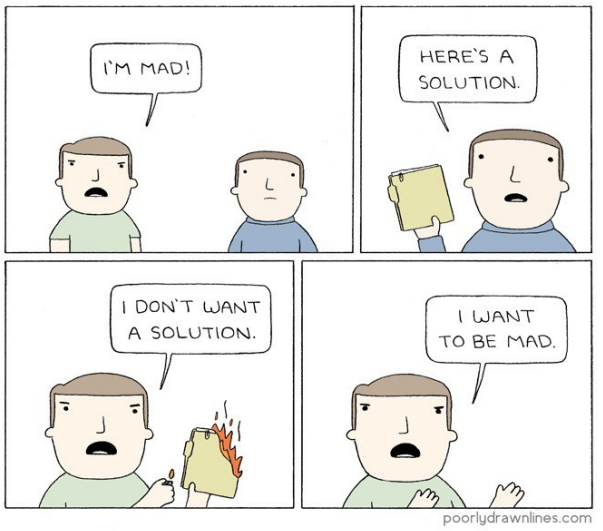
- What problems do you run into in your day-to-day work? Is there a standard way of solving it, or do you have a workaround?
  - Why is this a problem? How do you solve the problem today? How would you ideally like to solve the problem?
- Keep asking follow-up questions ("What else is a problem for you?", "Are there other things that give you trouble?") for as long as the interviewee has more problems to describe

Example: Identifying Problems (2)

- So, as I understand it, you are experiencing the following problems/needs …
  - Describe the interviewee's problems and needs in your own words: often **you do not share** the same image. It is very very common to not understand each other even if at first you think you do.
- Just to confirm, have I correctly understood the problems you have with the current solution?
  - Are there any other problems you're experiencing? If so, what are they?

Interview Tradeoffs

- Strengths
  - Reveal what stakeholders do, feel, prefer
  - How they interact with the system
  - Challenges with current systems
- Weaknesses
  - Subjective, yield inconsistencies
  - Hard to capture domain knowledge
  - Organizational issues, such as politics
  - Hinges on interviewer skill



Capturing and Synthesizing

- We acquire requirements from many sources
  - Elicit from stakeholders
  - Extract from policies or other documentation
  - Synthesize from above: estimation and invention
- Stakeholders do not always know what they want (!)
  - Be faithful to stakeholder needs and expectations
  - Anticipate additional needs and risks
  - Validate that “additional needs” are necessary or desired

Analogy: Ethnography

(Dr. Margaret Mead in Samoa, 1975)

Observation and Ethnography

- Observe people using their current system
- Passive: no interference with task performers
  - Watch from outside, record (notes, video), edit transcripts, interpret
  - Protocol analysis: they concurrently explain it
- Active: you get involved in the task, even become a team member
- Ethnographic studies, over long periods of time, discover emergent properties of social group involved

Mead vs. Freeman (1)

- In her popular 1928 book, *Coming of Age in Samoa*, Mead presented Samoan culture as a social system that allowed many adolescents to experiment sexually before marriage
  - Based on observations, interviews, ethnographic studies, etc.
- Mead almost certainly had a political agenda (she was a sexual progressive, etc.)
  - But that did not make her wrong

Mead vs. Freeman (2)

- In 19***83***, Freeman's *Margaret Mead and Samoa: The Making and Unmaking of an Anthropological Myth*, suggested that Mead was just gullible. Two of her informants had been lying: “Never can giggly fibs have had such far-reaching consequences in the groves of Academe.”
  - This significantly discredited her work
- It seemed his follow-on interviews found very different results. How could that be?

Mead vs. Freeman (3)

- Basically, *Freeman* was lying
- In 1996, Orans used Mead's own notes to show that “such humorous fibbing could not be the basis of Mead's understanding. Freeman asks us to imagine that the joking of two women, pinching each other as they put Mead on about their sexuality and that of adolescents, was of more significance than the detailed information she had collected throughout her fieldwork.”

Mead vs. Freeman (4)

- In 2011, Shankman used Freeman's own notes and found that his interviews were conducted in problematic ways:
  - “The 1987 interview with Fa'apua'a was arranged and carried out by Fofoa's son, a Samoan Christian of high rank who was convinced that Mead had besmirched the reputation of Samoans by portraying his mother, her friend Fa'apua'a, and other Samoans as sexually licentious.”
  - “Fofoa's son told Fa'apua'a "that the purpose of the interview was to correct 'the lies she [Mead] wrote in her book, lies that insult you all.'"”

Mead vs. Freeman (5)

- Shankman notes that “there is no information on the sex from these two women in Mead's field notes”: she could not have been fooled by women who were not her informants
  - Instead, she drew her conclusions from data on 25 adolescent girls, of whom over 40% were sexually active, and interviews with men and women
- While she may have downplayed some aspects of Samoan sexuality (e.g., rape and physical punishment for those who violated norms), she did not invent a false narrative

Requirements Interviews vs. Ethnography

- Discuss: why I am telling you so much about ethnography and cultural anthropology?
- What are two RE situations that might have similar issues?

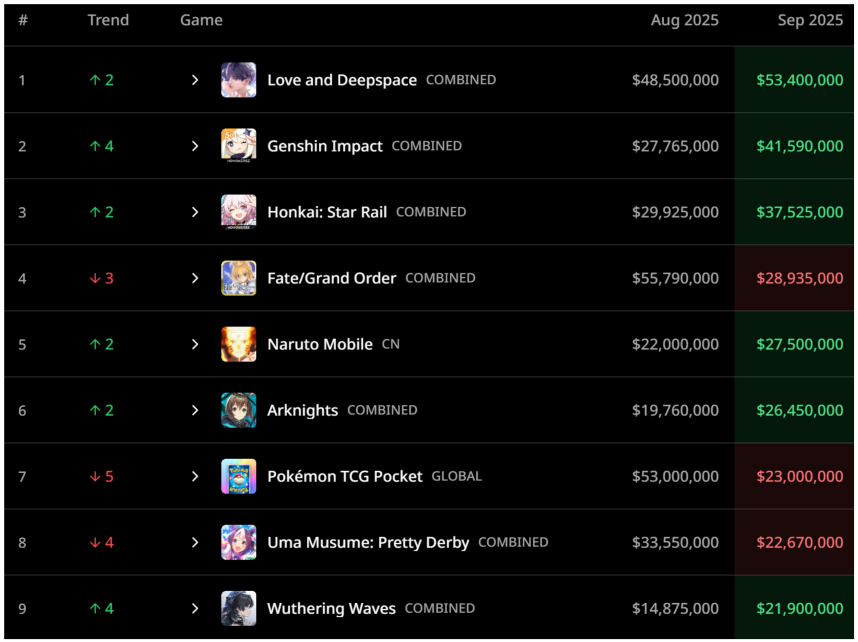
Want to read more? Try "Sex, Lies, and Separating Science From Ideology":
https://www.theatlantic.com/health/archive/2013/02/sex-lies-and-separating-science-from-ideology/273169/

Trivia: Western Philosophy

- Identify the philosopher associated with each quote:
- “Man is by nature a political animal.” (~350 BCE)
- “All human knowledge begins with intuitions, proceeds from thence to concepts, and ends with ideas.” (1781)
- “More natural is our position in politics: We see problems of power, of one quantum of power against another. We do not believe in any right that is not supported by the power of enforcement: we feel all rights to be conquests.” (1888)
- “It is nonsense to assert that revelry, vice, ecstasy, passion, would become impossible if man and woman were equal in concrete matters.” (1949)

Trivia: Video Games

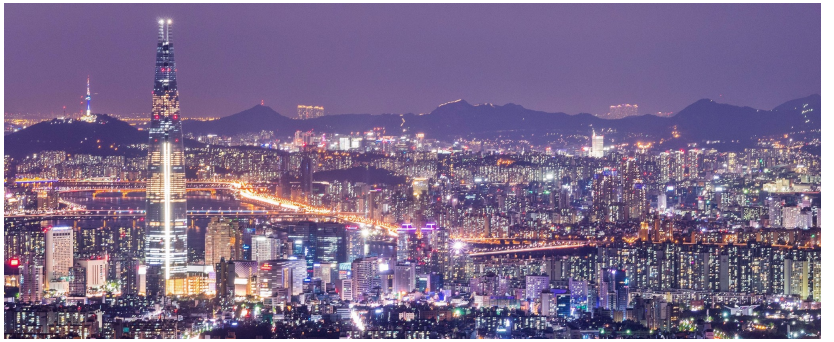
- This gambling-adjacent video game genre features a “vending machine” or “loot box” mechanic in which real and in-game currencies are spent to receive in-game “items” of varying rarity. It is named for the sound made by hand-cranked toy capsule vending machines.



#	Trend	Game	Aug 2025	Sep 2025
1	↑ 2	Love and Deepspace COMBINED	$48,500,000	$53,400,000
2	↑ 4	Genshin Impact COMBINED	$27,765,000	$41,590,000
3	↑ 2	Honkai: Star Rail COMBINED	$29,925,000	$37,525,000
4	↓ 3	Fate/Grand Order COMBINED	$55,790,000	$28,935,000
5	↑ 2	Naruto Mobile CN	$22,000,000	$27,500,000
6	↑ 2	Arknights COMBINED	$19,760,000	$26,450,000
7	↓ 5	Pokémon TCG Pocket GLOBAL	$53,000,000	$23,000,000
8	↓ 4	Uma Musume: Pretty Derby COMBINED	$33,550,000	$22,670,000
9	↑ 4	Wuthering Waves COMBINED	$14,875,000	$21,900,000

Trivia: Countries

- This country unified from three kingdoms into a singular political entity in 676. It gave rise to the world's first metal movable type (13th century) and a lovely constructed alphabet (15th century), but was weakened by Mongol invasions and annexation by Japan. Its largest city is the fourth most economically powerful in the world, measured by GDP.



Identifying Conflicts: Inconsistencies

- Terminology clash: same concept named differently in different statements
  - e.g., library: “borrower” vs. “patron”
- Designation clash: same name for different concepts in different statements
  - e.g., “user” for “library user” vs. “library software user”
- Structure clash: same concept structured differently in different statements
  - e.g., “latest return date” as time point (e.g. Fri 5pm) vs. time interval (e.g. Friday)

Conflict Strength

- In a **strong conflict**, statements are not satisfiable together
  - e.g., “participant constraints may not be disclosed to anyone else” vs. “the meeting initiator must know participant constraints”
- In a **weak conflict** (**divergence**), statements are not satisfiable together under some boundary condition
  - e.g., “patrons shall return borrowed copies within *X* weeks” vs “patrons may keep borrowed copies as long as needed” contradicts only if “needed>*X*”

Contracts “In Real Life”

190 F. Supp. 116 (1960)

FRIGALIMENT IMPORTING CO., Ltd., Plaintiff,
v.
B.N.S. INTERNATIONAL SALES CORP., Defendant.

United States District Court S. D. New York.

December 27, 1960.

***117** Riggs, Ferris & Geer, New York City (John P. Hale, New York City, of counsel), for plaintiff.

Sereni, Herzfeld & Rubin, New York City (Herbert Rubin, Walter Herzfeld, New York City, of counsel), for defendant.

FRIENDLY, Circuit Judge.

The issue is, what is chicken? Plaintiff says "chicken" means a young chicken, suitable for broiling and frying. Defendant says "chicken" means any bird of that genus that meets contract specifications on weight and quality, including what it calls "stewing chicken" and plaintiff pejoratively terms "fowl". Dictionaries give both meanings, as well as some others not relevant here. To support its, plaintiff sends a number of volleys over the net; defendant essays to return them and adds a few serves of its own. Assuming that both parties were acting in good faith, the case nicely illustrates Holmes' remark "that the making of a contract depends not on the agreement of two minds in one intention, but on the agreement of two sets of external signsnot on the parties' having *meant* the same thing but on their having *said* the same thing." The Path of the Law, in Collected Legal Papers, p. 178. I have concluded that plaintiff has not sustained its burden of persuasion that the contract used "chicken" in the narrower sense.

https://law.justia.com/cases/federal/district-courts/FSupp/190/116/1622834/

Resolving Conflicts

- "No Silver Bullet" (this is why they pay you)
- For Terminology, Designation and Structural conflicts: build a glossary
- For Weak and Strong Conflicts: negotiation is typically required
  - If the cause is different stakeholder objectives, it must be resolved outside of RE
  - If the cause is quality desires (e.g., "Good, cheap, on-time: pick two"), you explore quality tradeoffs

Step 4: Explore Alternatives

- Alternative solutions and tradeoffs are typically presented via **prototypes**, **mockups** or **storyboards**
- Mockups can be low- or high-fidelity
- Rapid prototypes can be throw-away (designed to learn about the problem, not for actual use) or evolutionary (intended to be incorporated into the final product)
- Stories detail who the players are, what happens to them, how it happens, why it happens, and what could go wrong

Informality

- Storyboards and mockups definitely do exist, but are often informal and incomplete

Exploration

- Humans are better at recognizing and evaluating solutions than facing blank pages
- Mockups and prototypes explore uncertainty in requirements
  - Validate that we have the right requirements
  - Get feedback on a candidate solution
  - “I'll know it when I see it.”
- Stories illuminate the system by walking through real or hypothetical sequences

Requirements Documentation

- Formal standards for writing down requirements exist (e.g., “may” vs. “must) but are not a focus for this course
  - They vary by domain and company (e.g., startup vs. established)

At last, he has found the famous Requirements Document dating back to the Traditional Age.

Requirements Elicitation: Reminder

- **Requirements elicitation** is the process of identifying system requirements through communication with stakeholders. Typically:

  Step 1. Identify stakeholders

  Step 2. Understand the domain

  - Analyze artifacts, interact with stakeholders

  Step 3. Discover the real needs

  - Interview stakeholders, resolve conflicts

  Step 4. Explore alternatives to address needs

Risks

- We want to mitigate **risk**, any uncertain factor that may result in a loss of satisfaction of a corresponding objective
- For example:
  - The system delivers a radiation overdose to patients (Therac-25, Theratron-780)
  - Medication administration record (MAR) knockout (provided inaccurate medication plans hospital-wide)
  - Premier Election Solutions vote-dropping “glitch”

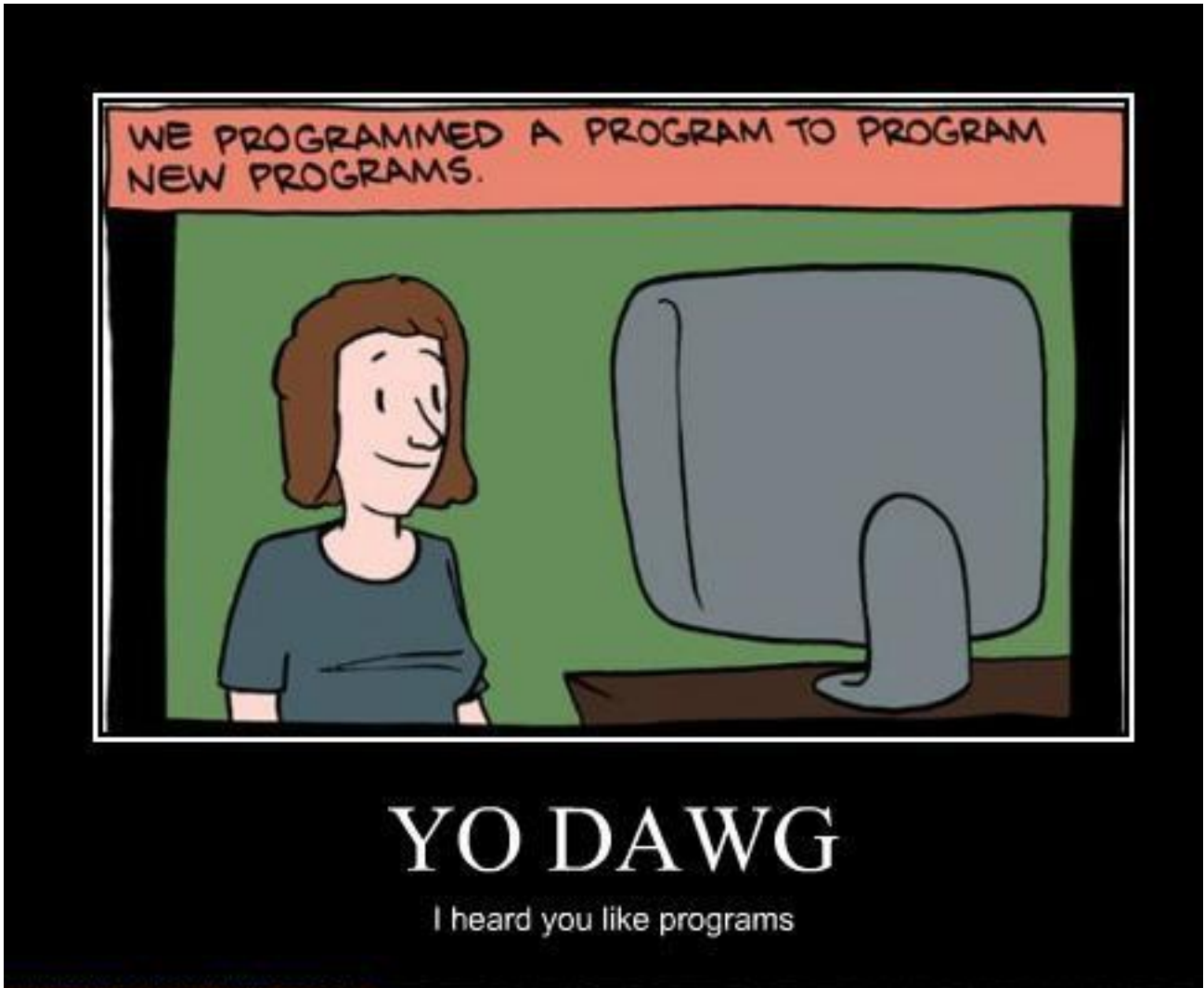
Risk Assessment

- Risk consists of multiple parts:
  - The likelihood of failure
  - The negative consequences or impact of failure
  - In advanced models: the causal agent and weakness
- Mathematically,

  Risk = Likelihood · Impact

Requirements for Requirements (to mitigate risk)

- Correct
- Consistent
- Unambiguous
- Complete
- Feasible
- Relevant
- Testable
- Traceable



Verification and Validation

- **Validation** is the task of determining if the requirements are correct
  - Are the requirements complete? Do they reflect the client's problem? Are they consistent?
- **Verification** is the task of determining if the software is correct (e.g., by testing)
  - Does the software satisfy the specification?
  - Is the specification correct with respect to the requirements, assuming the domain properties hold?

Approaches

Validation

- Interviews
- Reading
- Walkthroughs
- Prototypes
- Scenarios
- Checklists
- Modeling

Verification

- Testing
- Mathematical proofs
- Simulation
- Static analysis
- Dynamic analysis
- Checks for unreachable states or transitions (model checking)

Decomposition

- We recursively **decompose** a system, from the highest level of abstraction (stakeholder requirements) into lower-level subsystems and implementation choices
- This decomposition establishes **traceability**, which identifies relationships between requirements and implementations
- Traceability is important for verification and when requirements change
- Decomposition helps both validate and verify

Fault Tree Analysis

- **Fault tree analysis** is a top-down modeling technique to model, reason about, and analyze risk
- A fault tree analysis decomposes a particular type of failure into constituent potential causes (and probabilities)
- It defines the scope of system responsibilities and identifies unacceptable risk conditions that should be mitigated
- See https://mlip-cmu.github.io/book/07-planning-for-mistakes.html#fault-tree-analysis

Partial Fault Tree Analysis

"for the system failure of trapping a person in the door of an autonomous train"

Notation:

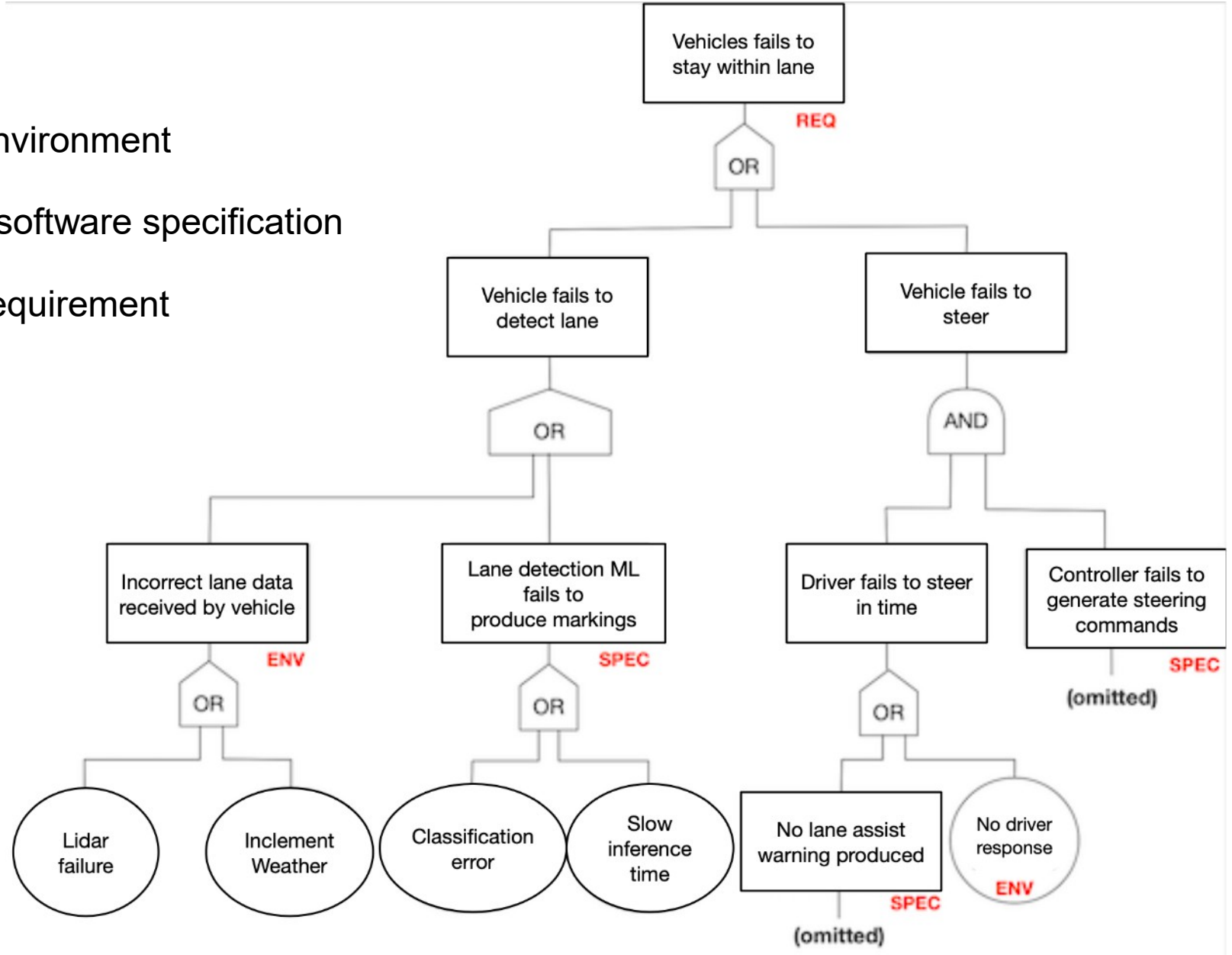
- Event
- Basic event (not decomposed)
- OR — OR connector
- AND — AND connector

ASM = assumption violation
SPEC = software specification violation
REQ = requirement violation

Fault Tree Analysis Example

"the vehicle must be prevented from veering out of the lane"

ENV = environment violation
SPEC = software specification violation
REQ = requirement violation

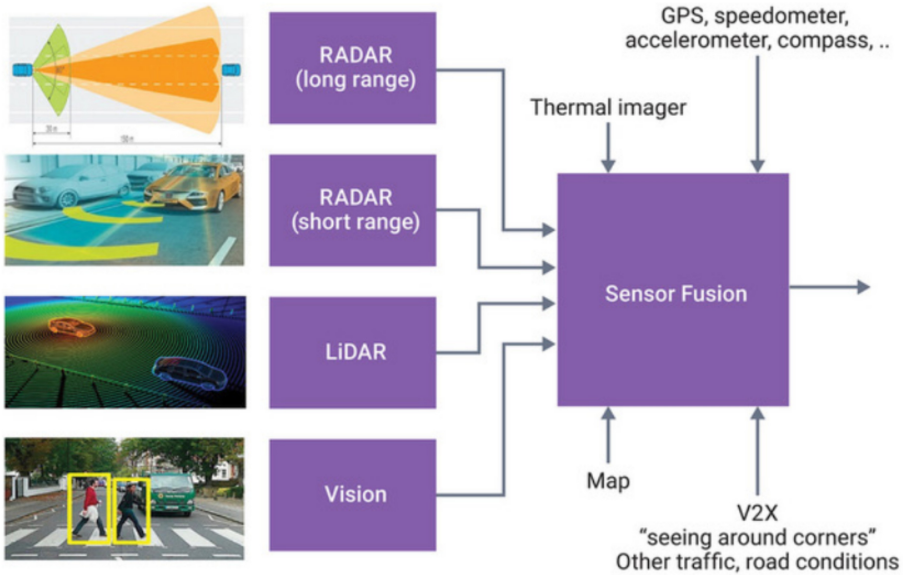


Risk Response Strategies

- Accept the risk: for low likelihood or low impact risks, or where the cost of mitigation is too high
- Transfer the risk: push the risk outside the system boundary
- Mitigate the risk: introduce active countermeasures
  - Reduce likelihood of failure; reduce severity of impact; change *or*s to *and*s!
- Avoid the risk: redesign so that risk cannot occur

Example Mitigation: Sensor Fusion

- Replace a single sensor node with a combination of multiple sensors
  - "violation if X fails" → "violation if X fails **and** Y fails"
- This can provide partial information even when one sensor is faulty
- A critical model for modern self-driving cars



Fault Tree Practice

- Requirement: the music that is selected to play on the front page of the website must not contain hate speech lyrics
- With your team …
  - Draw a simple fault tree analysis
  - Must contain one “software specification violation” node and one other type of violation
  - Link one risk mitigation to a particular node

Questions?


I'LL DESIGN THE SYSTEM AS SOON AS YOU GIVE ME THE USER REQUIREMENTS.
www.dilbert.com scottadams@aol.com
BETTER YET, YOU COULD BUILD THE SYSTEM, THEN I'LL TELL YOUR BOSS THAT IT DOESN'T MEET MY NEEDS.
I DON'T MEAN TO FRIGHTEN YOU, BUT YOU'LL HAVE TO DO SOME ACTUAL WORK.
THAT'S CRAZY TALK.