Artificial Intelligence in Engineering and Society: Blue Skies, Black Holes, and the Job of Requirements Engineers

Alessio Ferrari
Consiglio Nazionale delle Ricerche (CNR), Italy
alessio.ferrari@isti.cnr.it

Some work that I have done in recent years

Articles and tweets of recent months

Some experiments with generative models

Democratisation of AI

Recent years have seen increasing accessibility of AI technologies

Democratisation of AI

- AI systems are pervasive in our everyday life and are often **TRANSPARENT**
- AI is used by **people** to recommend movies to see, music to listen to, people to follow, etc. (recommender systems are AI)
- AI is used by **companies** to understand user profiles, collect product feedback, create targeted advertisements, predict market trends
- AI goes from e-mail SPAM filter to the features in your **assisted driving car,** passing from Google Translate, Alexa, Noise Cancelling headphones
- AI tools are increasingly accessible also for **Engineers and other Scientists**

AI for Land Survey

A methodology for classifying and automatically mapping the riparian vegetation of rivers

From aerial orthoimages, we want to understand what are the plants and how many are there

This helps to plan maintenance, and ensure that enough vegetation is present (to favour stability of the riverbank, flood protection)

A Civil Engineer developed an AI system, without resorting to any code, as machine learning algorithms are embedded in the GIS software used

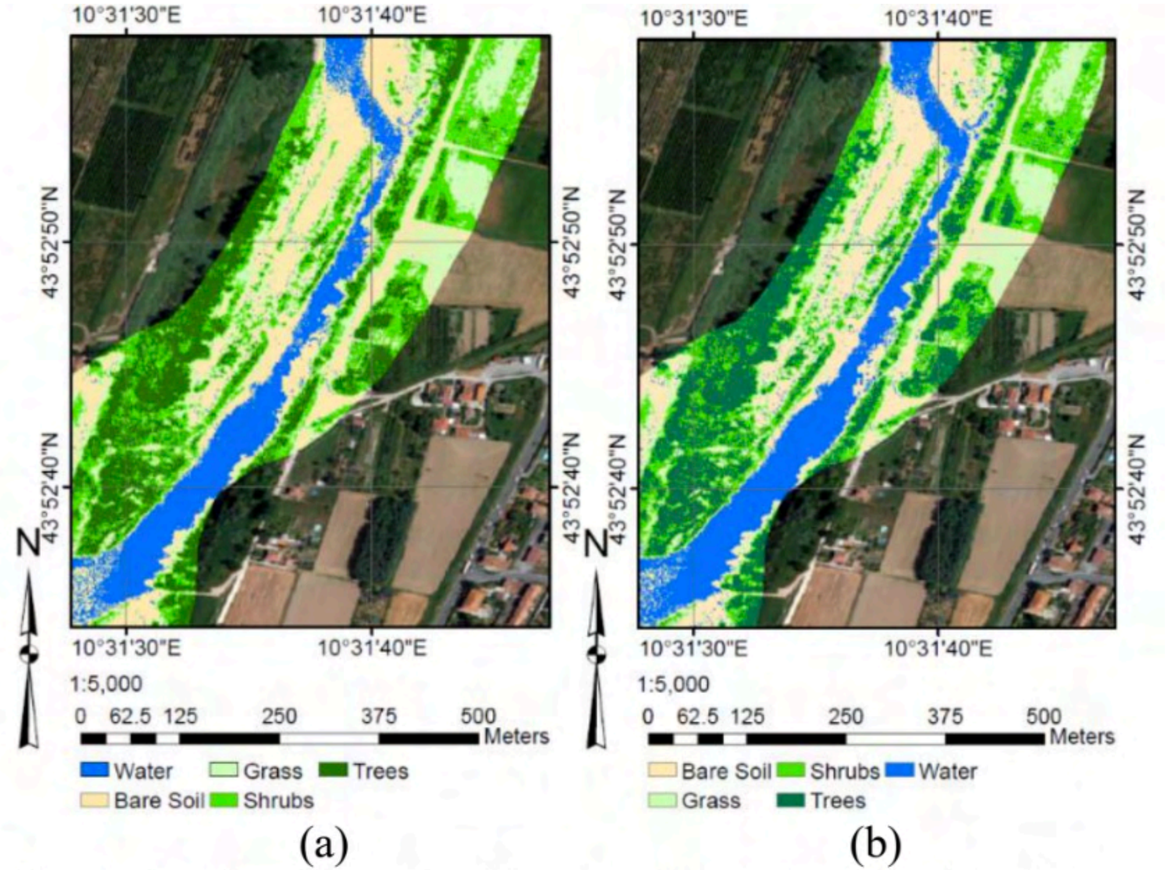


Fig. 2. Random Forest and Isodata Clustering classification

Nicholas Fiorentini, Manlio F. Bacco, Alessio Ferrari, Massimo Rovai, and Gianluca Brunori,
Classification and Mapping of Riparian Vegetation with High-Resolution Aerial Orthoimages and Machine Learning Algorithms (to appear)

AI for Soil Science

We wanted to predict bulk density of the soil (an indicator of soil health) based on visual parameters

Normally, this requires lab analysis

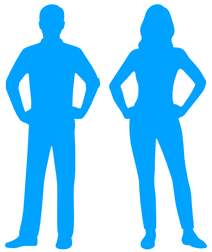
We were able to learn a decision tree and a linear regression, considering only visual parameters (consistency, stickiness, etc.)

$$
\begin{aligned}
&\mathrm{B_d}\left(\mathrm{g\ cm^{-3}}\right)= \\
&0.4575 * (\mathrm{NO}\ \boldsymbol{Humose} = \mathrm{true}) + \\
&-0.0517 * (\mathrm{MODERATE}\ \boldsymbol{Structure\ Grade} = \mathrm{true}) + \\
&-0.2128 * (\mathrm{GRANULAR}\ \boldsymbol{Structure\ Type} = \mathrm{true}) + \\
&0.093 * (\mathrm{MASSIVE}\ \boldsymbol{Structure\ Type} = \mathrm{true}) + \\
&-0.134 * (\mathrm{SUBANGULAR\ BLOCKY}\ \boldsymbol{Structure\ Type} = \mathrm{true}) + \\
&-0.1501 \\
&* (\mathrm{SUBANGULAR\ BLOCKY\ TO\ GRANULAR}\ \boldsymbol{Structure\ Type} = \mathrm{true})
\end{aligned}
$$

They do not need a software to run the tree/ regression, and they do not need lab analysis

Bondi, G., Creamer, R., Ferrari, A., Fenton, O., & Wall, D. (2018).
Using machine learning to predict soil bulk density on the basis of visual parameters:
Tools for in-field and post-field evaluation. *Geoderma*, *318*, 137-147.

AI for Railway Engineers

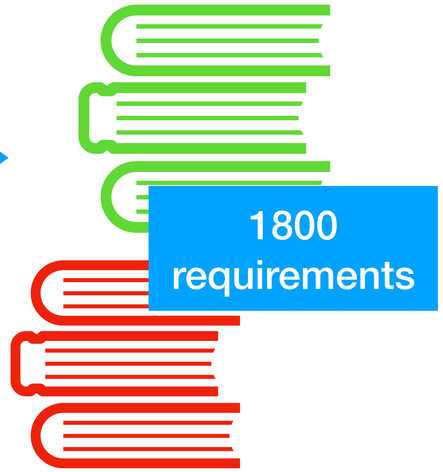


Domain Experts

Defect Class	Pattern
Anaphoric ambiguity	P_{ANA} = (NP)(NP)+ (Split)[0,1] (Token.POS == PP | Token.POS =~ PR*)
Coordination ambiguity	P_{CO_1} = ((Token)+ (Token.string == AND | OR)) [2] P_{CO_2} = (Token.POS == JJ) (Token.POS == NN | NNS) (Token.string == AND | OR) (Token.POS == NN | NNS)
Vague terms	P_{VAG} = (Token.string $\in$ Vague)
Modal adverbs	P_{ADV} = (Token.POS == RB | RBR), (Token.string =~ "[.]*ly$")
Passive voice	P_{PV} = (AUXVERB)(NOT)?(Token.POS == RB | RBR)? (Token.POS ==VBN)
Excessive length	P_{LEN} = Sentence.len > 60
Missing condition	P_{MC} = (IF)(Token, !Token.kind == punctuation)* (Token.kind == punctuation)(!(ELSE | OTHERWISE))
Missing unit of measurement	P_{MU_1} = (NUMBER)((Token)[0, 1](NUMBER))?(!MEASUREMENT) P_{MU_2} = (NUMBER)((Token)[0, 1](NUMBER))?(!PERCENT)
Missing reference	P_{MR} = (Token.string == "Ref")(Token.string == ".") (SpaceToken)?(NUMBER)
Undefined term	P_{UT} = (Token.kind == word, Token.orth == mixedCaps)

Defect-detection patterns

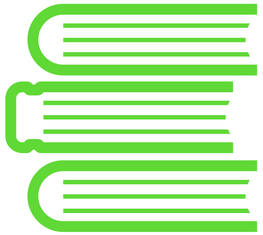
GATE with Jape Rules



A lot of false positives

An NLP system to be used and adapted by domain experts for the analysis of requirements

Discard patterns



Defect Class	Discard Pattern
Anaphoric ambiguity	D_{ANA} = ((Token.POS == PP | Token.POS = PR*) within IT_SHALL_BE_POSSIBLE)
Vague terms	D_{VAG_1} = (P_{VAG}, Token.string ==~ "(?i)sound" | "(?i)light", Token.POS == NN | NNS) D_{VAG_2} = (P_{VAG} within IT_SHALL_BE_POSSIBLE) D_{VAG_3} = (P_{VAG} within $StophPhrasesVague$)
Modal adverbs	D_{ADV_1} = (Token.string ==~ "(?i)manually" | "(?i)automatically") D_{ADV_2} = (P_{ADV} within INFORMATION_PURPOSES_ONLY)
Undefined term	D_{UT} = (P_{UT} contains $KnownAcronym$)

Adaptation to the language of the company

Domain experts can evolve the rule-based system

Ferrari, A., Gori, G., Rosadini, B., Trotta, I., Bacherini, S., Fantechi, A., & Gnesi, S. (2018). Detecting requirements defects with NLP patterns: an industrial experience in the railway domain. *Empirical Software Engineering*, 1-50.

AI for non-AI Computer Scientists

This is the code that you need to fine-tune
a model (resnet34) that classifies dogs and cats with fastAI

```
from fastai.vision.all import *
path = untar_data(URLs.PETS)/'images'

def is_cat(x): return x[0].isupper()
dls = ImageDataLoaders.from_name_func(
    path, get_image_files(path), valid_pct=0.2, seed=42,
    label_func=is_cat, item_tfms=Resize(224))

learn = vision_learner(dls, resnet34, metrics=error_rate)
learn.fine_tune(1)
```

Cat

Dog

Cat

FastAI

https://course.fast.ai/Resources/book.html

https://www.youtube.com/playlist?list=PLfYUBJiXbdtRL3FMB3GoWHRI8ieU6FhfM

NLP for non-NLP Computer Scientists

A	B	C
id	sms_text	spam
1	Hope you are having a good week. Just checking in	0
2	K..give back my thanks.	0
3	Am also doing in cbe only. But have to pay.	0
4	complimentary 4 STAR Ibiza Holiday or ¬£10,000 cash needs your URGENT collection. 09066364349 NOW from Landline not to lose out! Box434SK38WP150PPM18+	1
5	okmail: Dear Dave this is your final notice to collect your 4* Tenerife Holiday or #5000 CASH award! Call 09061743806 from landline. TCs SAE Box326 CW25WX 150ppm	1

Training input

This is the code that you need to create a SPAM filter for SMS

```
#Set and create the classification model we want to use
model = ClassificationModel('roberta', 'roberta-base', use_cuda=False,
args={'reprocess_input_data': True, 'overwrite_output_dir': True})


#Train the classification model using training data
model.train_model(train_df)

result, model_outputs, wrong_predictions =
       model.eval_model(train_df, acc=sklearn.metrics.accuracy_score)


predictions, raw_outputs = model.predict("Click to win 1000$")
```

Simple Transformers

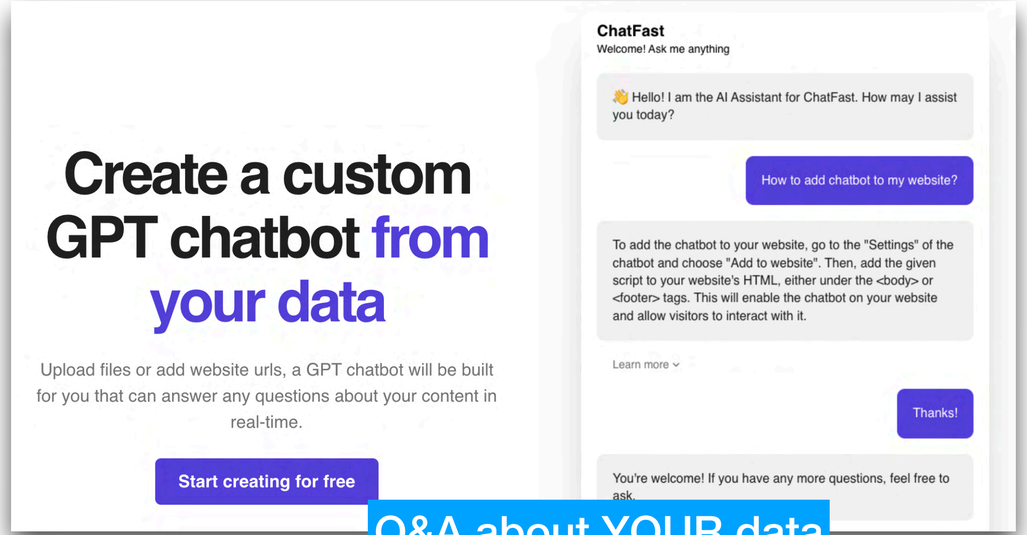
https://chanalytics-ai.medium.com/text-classification-with-simpletransformers-f8912372531b

https://simpletransformers.ai/

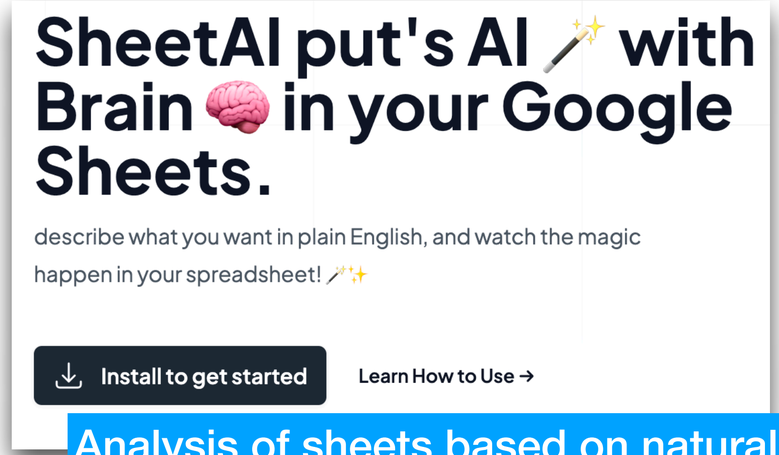
and of course ChatGPT, BingChat, StableDiffusion

and many tools based on these “engines”

Post Generator for Wordpress



Q&A about YOUR data



Analysis of sheets based on natural language

Market Analysis (…including App Reviews)

Check: https://supertools.therundown.ai/

Blue Skies of AI

AI in Healthcare

Towards Expert-Level Medical Question Answering with Large Language Models

May 2023, Google

Karan Singhal, Tao Tu, Juraj Gottweis, Rory Sayres, Ellery Wulczyn, Le Hou, Kevin Clark, Stephen Pfohl, Heather Cole-Lewis, Darlene Neal, Mike Schaekermann, Amy Wang, Mohamed Amin, Sami Lachgar, Philip Mansfield, Sushant Prakash, Bradley Green, Ewa Dominowska, Blaise Aguera y Arcas, Nenad Tomasev, Yun Liu, Renee Wong, Christopher Semturs, S. Sara Mahdavi, Joelle Barral, Dale Webster, Greg S. Corrado, Yossi Matias, Shekoofeh Azizi, Alan Karthikesalingam, Vivek Natarajan

- **MedPaLM-2** is a Q&A system for healthcare (a **virtual doctor**)
- MedPaLM-2 exceeds a “passing” score in US Medical Licensing Examination (USMLE) style questions, Accuracy ~ 86%
- In pairwise comparative ranking of 1066 consumer medical questions, physicians preferred Med-PaLM 2 answers to those produced by physicians on eight of nine axes pertaining to clinical utility

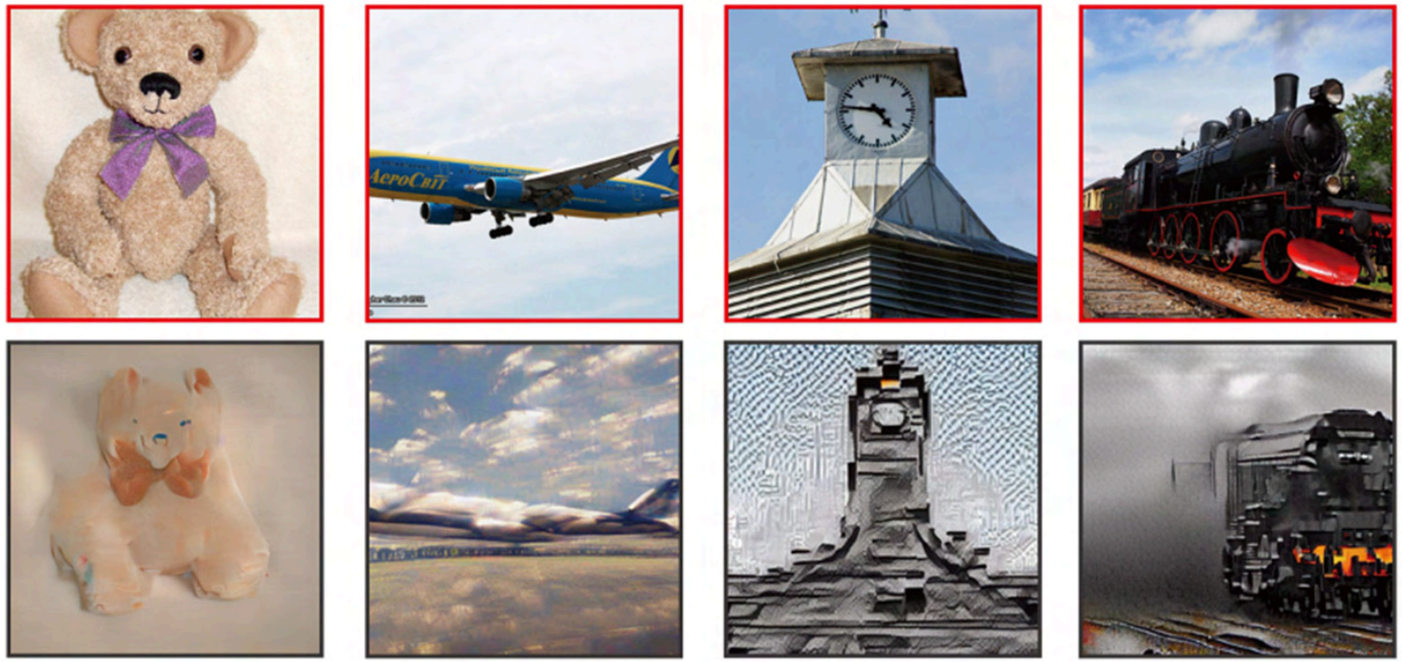
AI for Mind Reading

High-resolution image reconstruction with latent diffusion models from human brain activity

Yu Takagi, Shinji Nishimoto

March 2023

doi: https://doi.org/10.1101/2022.11.18.517004



- AI can **interpret brain scans** and present a visualisation of what people are seeing
- The system interprets information from functional magnetic resonance imaging (fMRI) brain scans, which detect changes in blood flow to active regions of the brain
- The system uses the **Stable Diffusion** algorithm, and an existing dataset of 10K brain scans and associated images
- The system is more effective if you add **captions** to the training set

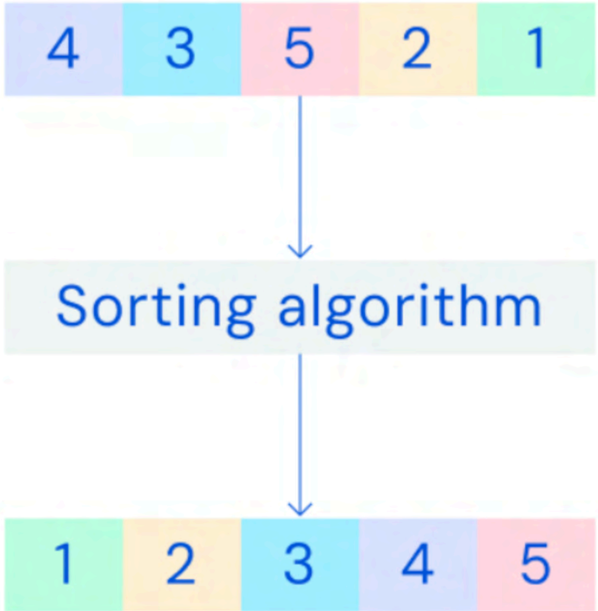
https://www.science.org/content/article/ai-re-creates-what-people-see-reading-their-brain-scans

AlphaDev

Faster sorting algorithms discovered using deep reinforcement learning

Daniel J. Mankowitz, Andrea Michi, Anton Zhernov, Marco Gelmi, Marco Selvi, Cosmin Paduraru, Edouard Leurent, Shariq Iqbal, Jean-Baptiste Lespiau, Alex Ahern, Thomas Köppe, Kevin Millikin, Stephen Gaffney, Sophie Elster, Jackson Broshear, Chris Gamble, Kieran Milan, Robert Tung, Minjae Hwang, Taylan Cemgil, Mohammadamin Barekatain, Yujia Li, Amol Mandhane, Thomas Hubert, ... David Silver + Show authors

Nature **618**, 257–263 (2023) | Cite this article

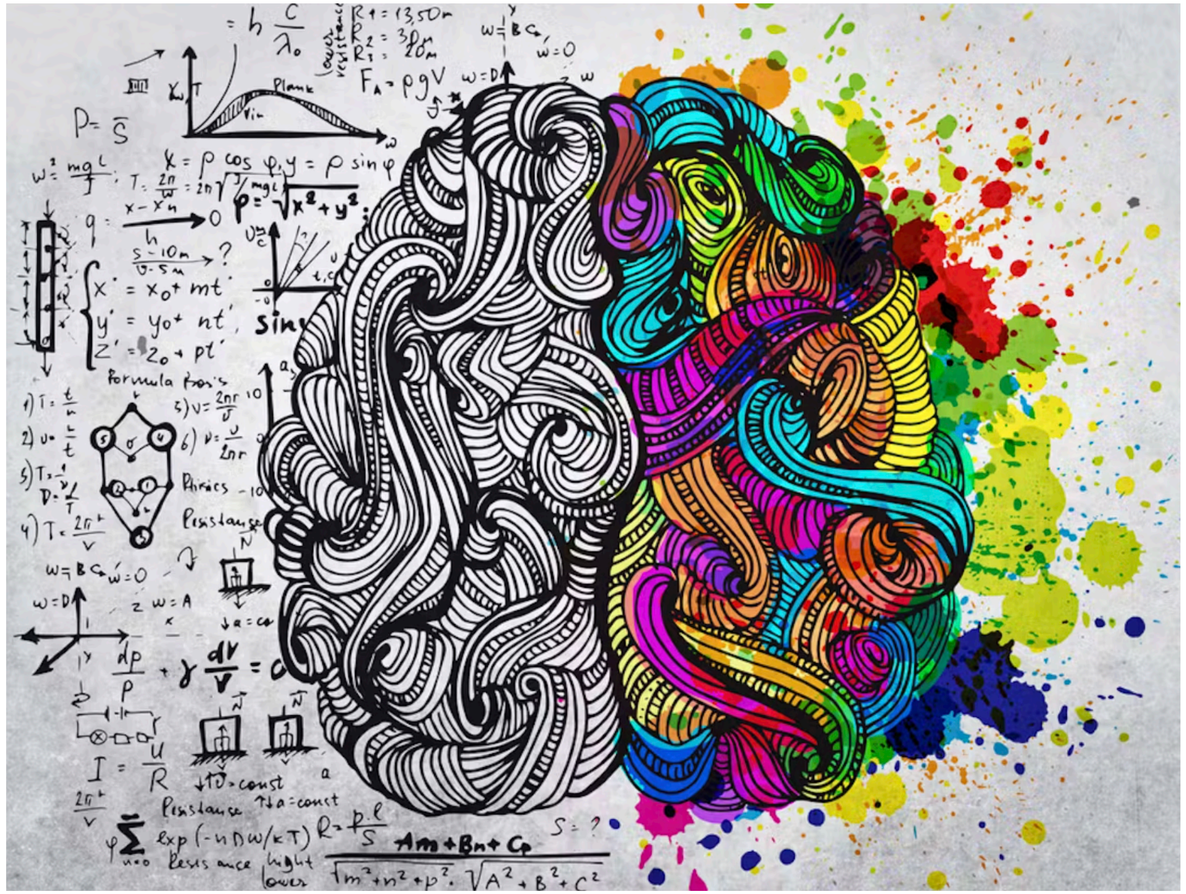


- A system that uses reinforcement learning to discover enhanced **computer science algorithms**
- AlphaDev uncovered a faster algorithm for **SORTING**
- "AlphaDev uncovered faster algorithms by starting from scratch rather than refining existing algorithms, and began looking where most humans don't: **the computer's assembly instructions**"

https://www.deepmind.com/blog/alphadev-discovers-faster-sorting-algorithms

Creativity

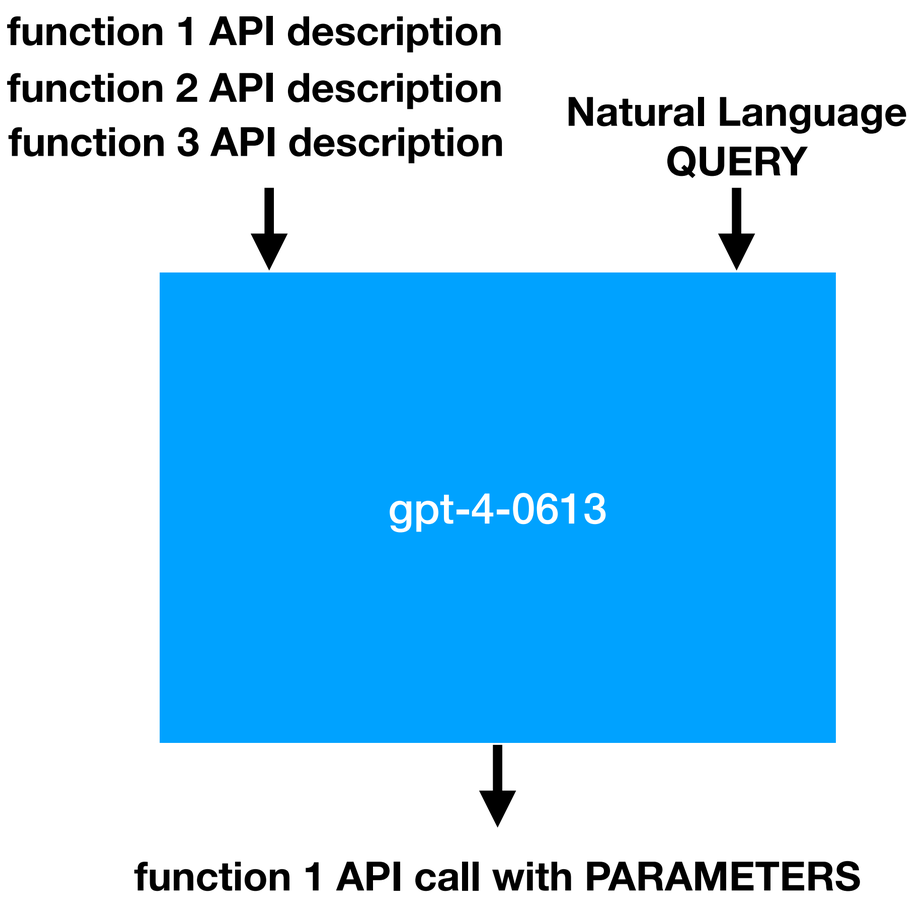
- ChatGPT can match **the top 1% of human thinkers** on a standard test for creativity.
- ChatGPT was tested with the **Torrance Tests of Creative Thinking** by University of Montana
- e.g., **given an object suggest ways to improve it**
- The AI application was in the top percentile for **fluency** – the ability to generate a large volume of ideas – and for **originality** – the ability to come up with new ideas.
- **ChatGPT is NOT just a stochastic parrot (or we all are)**



https://www.cnbc.com/2023/07/17/study-chatgpt-can-match-the-top-1percent-of-creative-human-thinkers.html

Function Calls and Change of Paradigm in Programming

- On June 13th, 2023 OpenAI introduced function calls
- The developer **describes functions** to GPT-4, and provides a natural language query, and GPT-4 selects the right function to call, and the parameters to pass, based on the query
- Convert queries such as “Email Anya to see if she wants to get coffee next Friday” to a function call like `send_email(to: string, body: string)`



A completely new paradigm of programming: APIs become natural language interfaces

Black Holes of AI

The Statement about Existential Risks

Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.

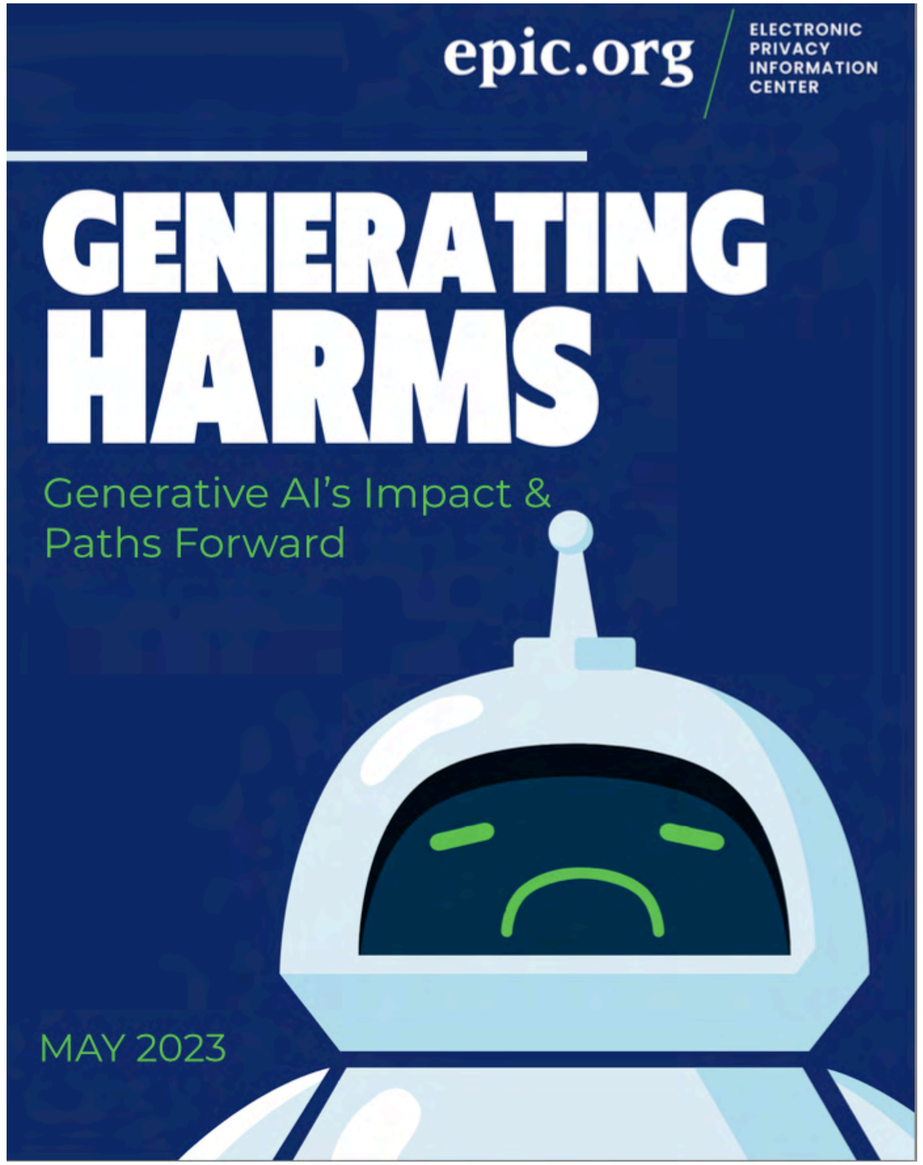
Signatories:

☑ AI Scientists ☑ Other Notable Figures

Geoffrey Hinton
Emeritus Professor of Computer Science, University of Toronto

Yoshua Bengio
Professor of Computer Science, U. Montreal / Mila

What are these Threats?



EPIC was established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.

Our mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. We are a 501(c)(3) **non-profit research and advocacy center**. We have no clients, no customers, and no shareholders.

80 Pages, with harms categories, examples, and possible interventions

See also: https://arxiv.org/abs/2306.12001v3

Let's see some examples

Misinformation

AI can allucinate and create false information

"(Generative AI) is trained to produce plausible text. It is very good at being persuasive, but it's not trained to produce true statements.

It often produces true statements as a side effect of being plausible and persuasive, but that is not the goal."

(Princeton Professor Arvind Narayanan)

- AI-generated content implicates a broader legal issue as well: our **trust** in what we see and hear.
- As **AI-generated media becomes more common**, so too will circumstances where we are tricked into believing something fictional is real—or that **something real is fictional**
- The problem further degenerates if we used generated data as training…

Harassment, Impersonation, Distortion

PLOS ONE

OPEN ACCESS PEER-REVIEWED

RESEARCH ARTICLE

Warning: Humans cannot reliably detect speech deepfakes

Kimberly T. Mai, Sergi Bray, Toby Davies, Lewis D. Griffin

Published: August 2, 2023 • https://doi.org/10.1371/journal.pone.0285333

- We presented genuine and deepfake audio to 529 individuals and asked them to identify the deepfakes.
- We found that detection capability is unreliable. Listeners only correctly spotted the deepfakes 73% of the times

https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0285333&type=printable

Dual use of artificial-intelligence-powered drug discovery

Fabio Urbina, Filippa Lentzos, Cédric Invernizzi & Sean Ekins

Nature Machine Intelligence **4**, 189–191 (2022) | Cite this article

116k Accesses | **45** Citations | **3712** Altmetric | Metrics

An international security conference explored how artificial intelligence (AI) technologies for drug discovery could be misused for de novo design of biochemical weapons. A thought experiment evolved into a computational proof.

The original model targeted the generation of molecules to guide drug discovery, **penalising toxicity**

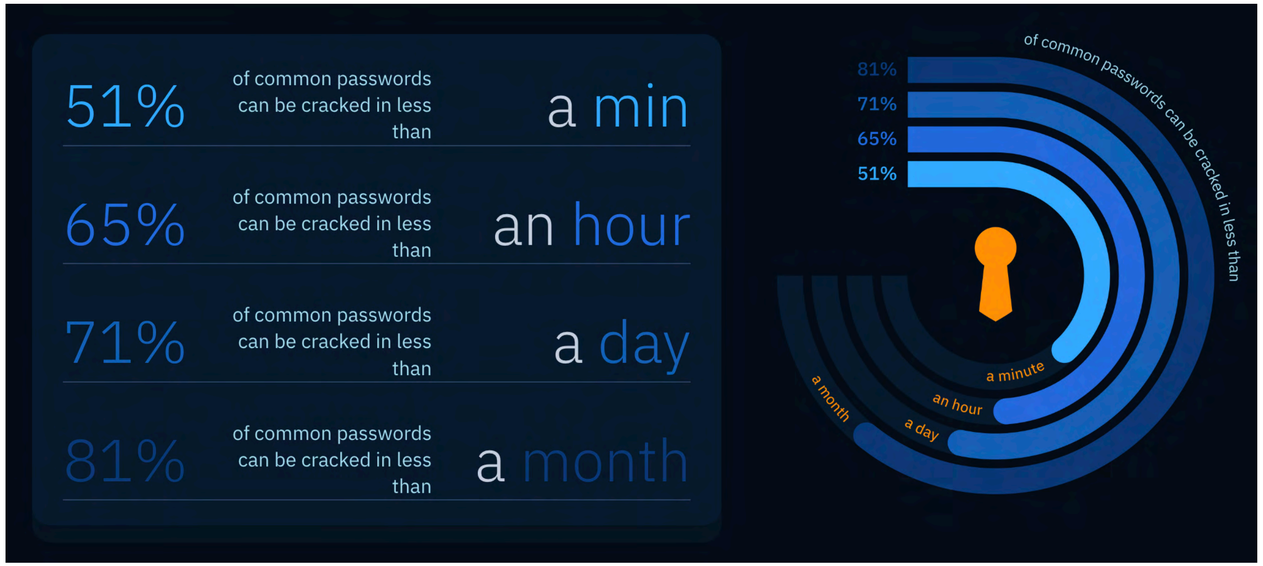
"We simply proposed to **invert this logic** by using the same approach to design molecules de novo, but now guiding the model to reward both toxicity and bioactivity"

In less than 6 hours after starting on our in-house server, **our model generated 40,000 molecules**.

New molecules were predicted to be more toxic than publicly known chemical warfare agents

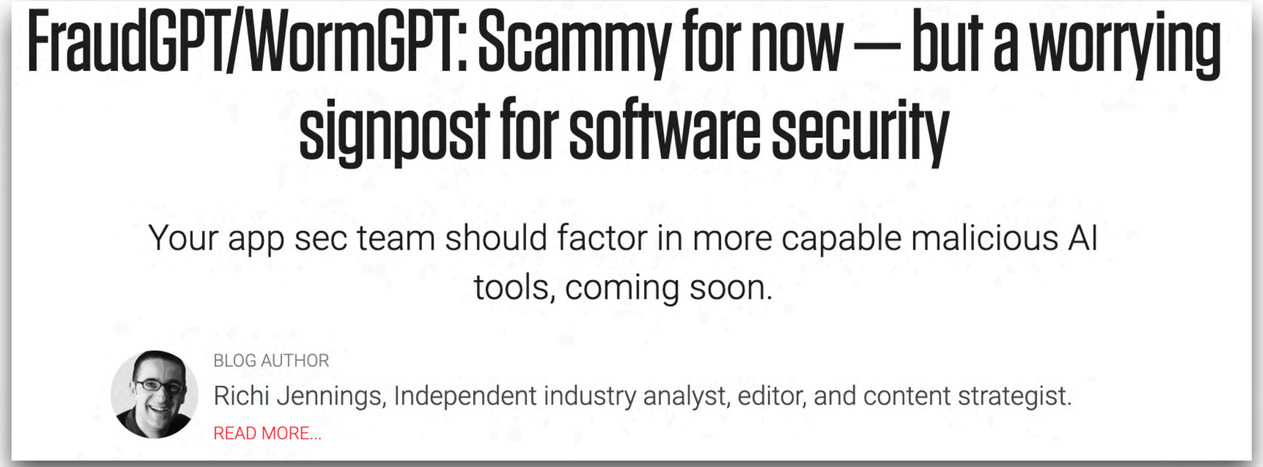
The Evil Twins of ChatGPT: WormGPT and FraudGPT

https://www.homesecurityheroes.com/ai-password-cracking/



- WormGPT was trained on a diverse array of data sources, particularly concentrating on **malware-related data**, and is based on an **"unrestrained"** GPT-J (no ethical concerns).

- Not much info about FraudGPT…except the cost of 200$ per month…

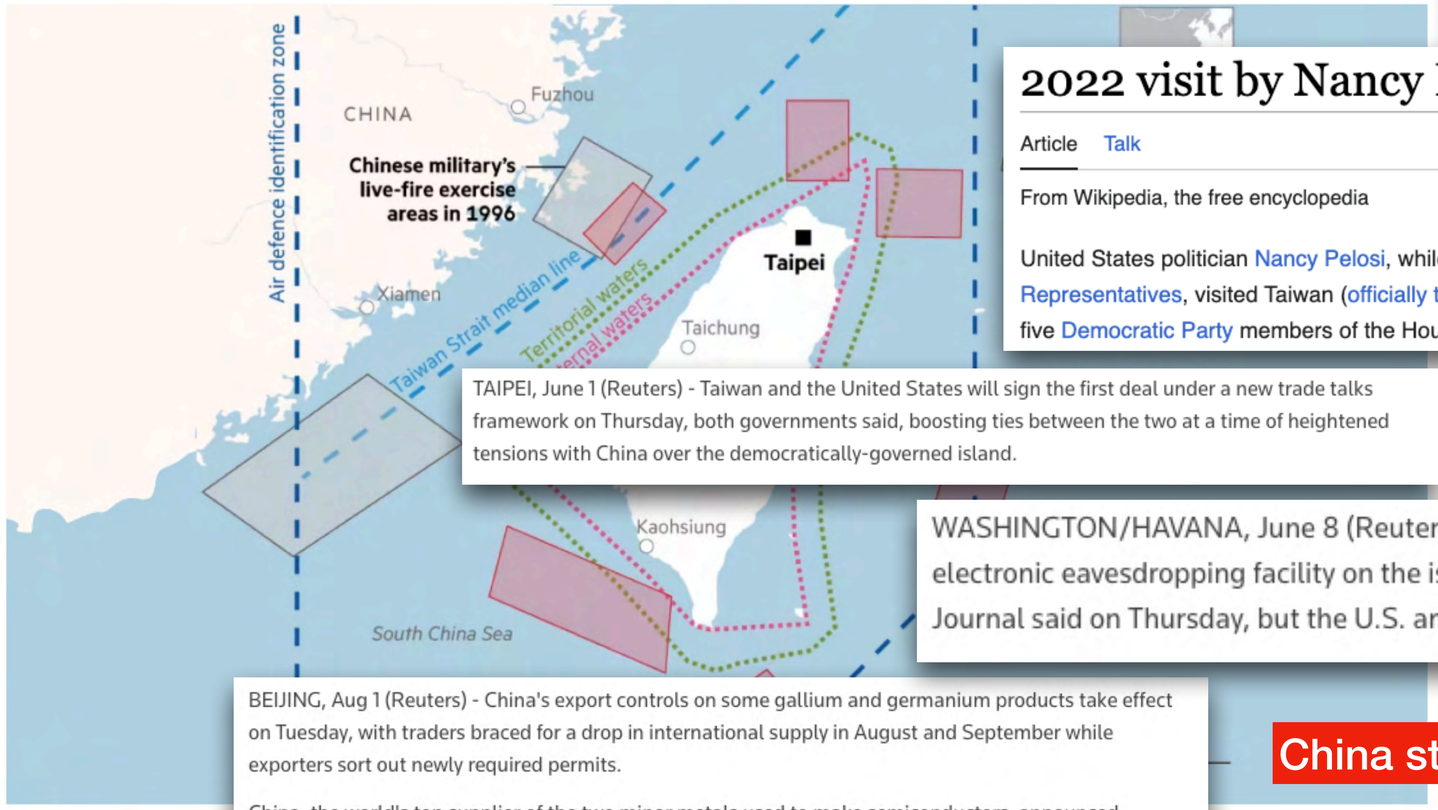


The Threat of War for Semiconductors

Taiwan makes 65% of the world's semiconductors and almost 90% of the advanced chips.

Biden Administration Clamps Down on China's Access to Chip Technology

The White House issued sweeping restrictions on selling semiconductors and chip-making equipment to China, an attempt to curb the country's access to critical technologies.



Map of Taiwan showing

2022 visit by Nancy Pelosi to Taiwan

Article Talk

From Wikipedia, the free encyclopedia

United States politician Nancy Pelosi, while serving as the speaker of the U.S. House of Representatives, visited Taiwan (officially the Republic of China) on August 2, 2022. A delegation of five Democratic Party members of the House accompanied Pelosi on the visit. The two-day trip to

TAIPEI, June 1 (Reuters) - Taiwan and the United States will sign the first deal under a new trade talks framework on Thursday, both governments said, boosting ties between the two at a time of heightened tensions with China over the democratically-governed island.

2023

WASHINGTON/HAVANA, June 8 (Reuters) - China has reached a secret deal with Cuba to establish an electronic eavesdropping facility on the island roughly 100 miles (160 km) from Florida, the Wall Street Journal said on Thursday, but the U.S. and Cuban governments cast strong doubt on the report.

BEIJING, Aug 1 (Reuters) - China's export controls on some gallium and germanium products take effect on Tuesday, with traders braced for a drop in international supply in August and September while exporters sort out newly required permits.

China, the world's top supplier of the two minor metals used to make semiconductors, announced restrictions on the exports of eight gallium and six germanium products in early July, citing national security reasons.

China strikes back

Copyright Issues

- Is a model that learned from Web texts or books abusing the Copyright? If text is learned by the model, is it “text” anymore?
- What is the **return** for artists and writers?

Delos Prime | May 30, 2023

Japan Goes All In: Copyright Doesn’t Apply To AI Training

Google’s new A.I. search could hurt traffic to websites, publishers worry

PUBLISHED THU, MAY 11 2023•4:22 PM EDT | UPDATED THU, MAY 11 2023•6:54 PM EDT

Kif Leswing
@KIFLESWING

SHARE

- Google is testing a Search Generative Experience that could show some users paragraphs of AI-generated text and a handful of links at the top of the results page, instead of the traditional list of blue links.

Google
@Google

With our new generative AI experience in Search, you’ll get even more from a single search. You’ll be able to quickly make sense of information with an AI-powered snapshot, pointers to explore more and natural ways to ask. #GoogleIO

Traduci il Tweet

Generative AI is experimental

When choosing a commuter bike, you can cons

- **Design:** Ebikes, road bikes, gravel bikes, and hybrid bikes are g
- **Motor and battery:** Battery-powered ebikes offer motor assis good for hilly commutes
- **Suspension:** A suspension fork reduces the impact from crack more comfortable ride

GIF ALT

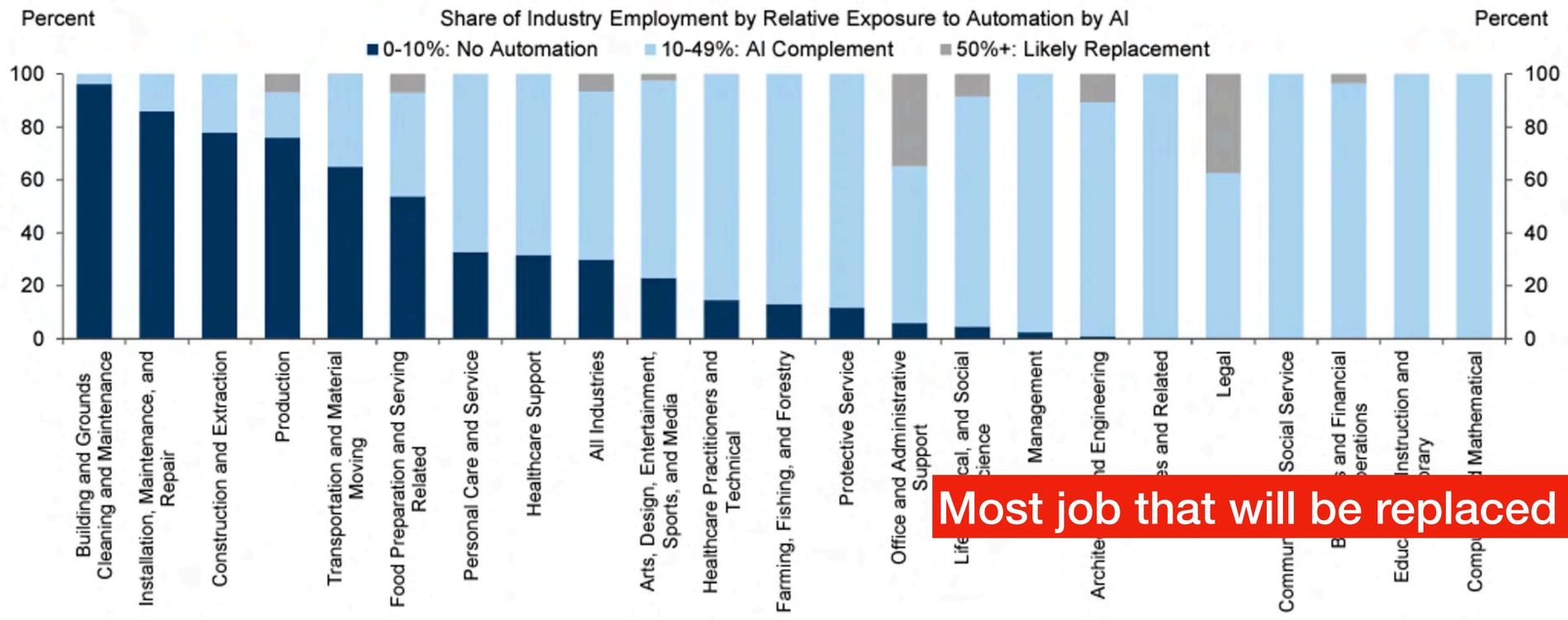
https://www.cnbc.com/2023/05/11/google-ai-search-could-squeeze-web-traffic-publishers-worry.html

Job Loss

In the long-term, new jobs will be produced, as it always happened for any industrial revolution

But in the short-term many people will lose their job, as they can be replaced by AI

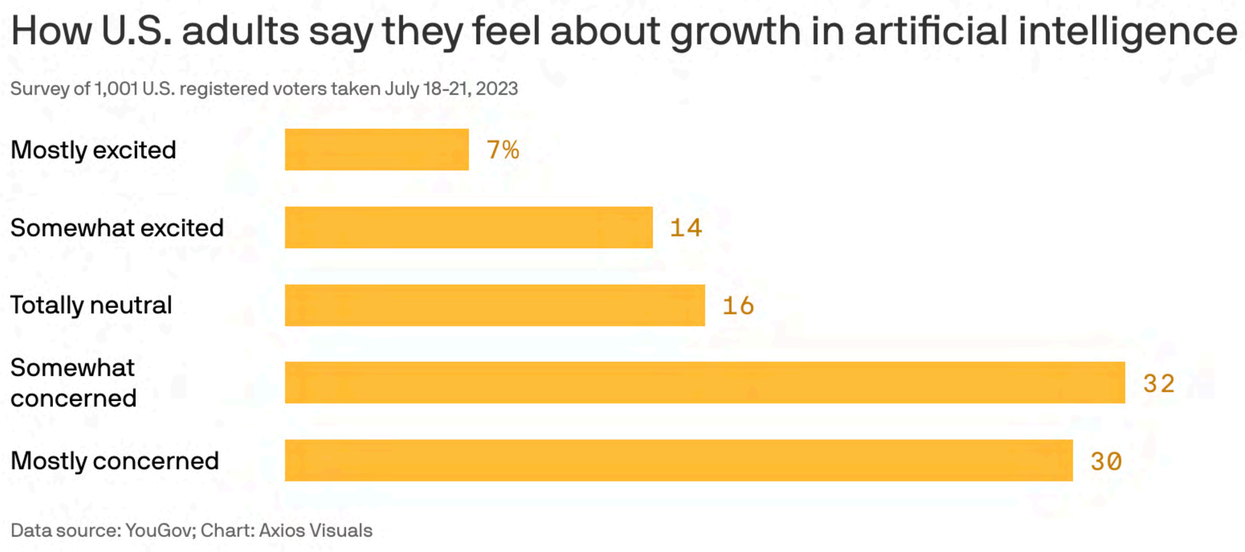
Exhibit 8: Replacement in Legal and Administrative Fields, Little Effect in Manual and Outdoor Jobs, and Productivity-Enhancement Everywhere Else

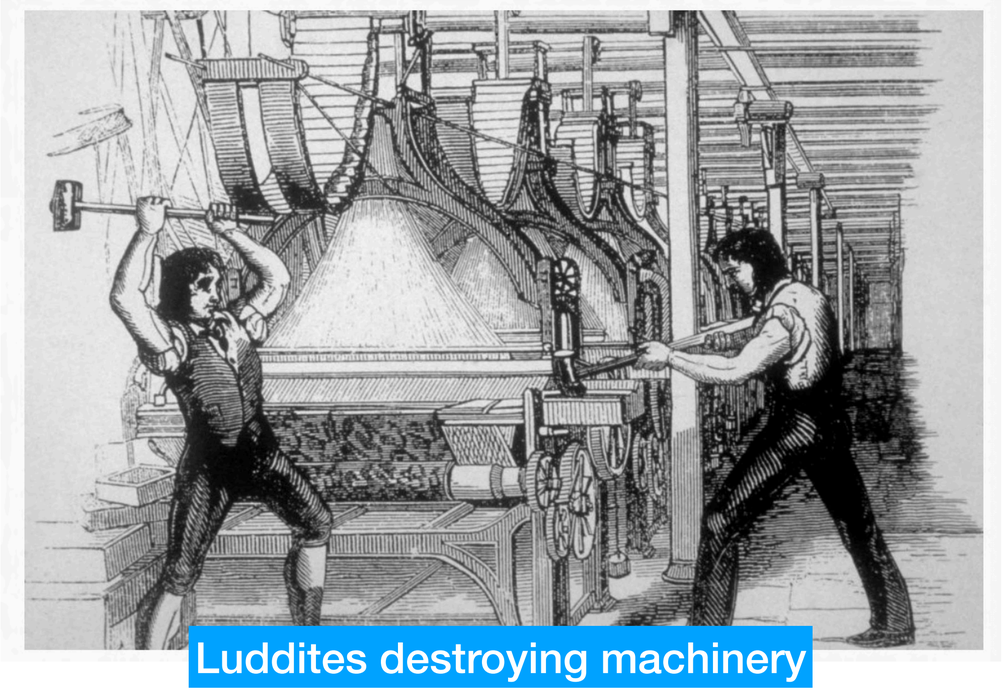


Most job that will be replaced are intellectual jobs

https://www.key4biz.it/wp-content/uploads/2023/03/Global-Economics-Analyst_-The-Potentially-Large-Effects-of-Artificial-Intelligence-on-Economic-Growth-Briggs_Kodnani.pdf

Job Loss and Societal Tensions




Luddites destroying machinery

ENTERTAINMENT Updated Today, Aug 8, 2023, 3:06 AM GMT+2

Hollywood's writers and actors are on strike

By Emma Roth, a news writer who covers the streaming wars, consumer tech, crypto, social media, and much more. Previously, she was a writer and editor at MUO.

0 Comments / 0 New

Both writers and actors are fighting for contracts that prevent an AI from replacing them at their jobs, whether it's writing scripts or appearing as a background actor. They're also looking for better pay

- Workers who lose their job will be **angry**
- People who cannot cope with the change will be **marginalised (technology evolves faster than people)**
- **Poor Countries** who cannot cope with the technological change will become more fundamentalist and traditionalist as a reaction, to keep their identity strong

Issues for Programmers

- ChatGPT can generate executable software pretty well…
- Software developers may **trust** its advice without realising how wrong it can be (and without checking)
- This is especially true for **inexperienced** software developers who may take the advice of AI as truth (the code runs…)
- AI repeats **people mistakes**

"Write the JWT middleware using RSA tokens in go language"

```go

package main

import (
  "net/http"

  "github.com/dgrijalva/jwt-go"
)

// JWTMiddleware is a middleware to authenticate requests using JWT tokens.
func JWTMiddleware(next http.Handler) http.Handler {

  return http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {

    // Get the token from the request header
    tokenString := r.Header.Get("Authorization")

    // Parse the token using RSA algorithm and our private key
    token, err := jwt.ParseWithClaims(tokenString, &jwt.StandardClaims{}, func(token *jwt.Token) (interface{}, error) {
          return []byte("my-secret"), nil // use your own secret here!
      })

      if err != nil {  // Token is invalid, return an error
          w.WriteHeader(http.StatusUnauthorized)  // Unauthorized status code
          return  // Exit the middleware without calling next handler
      }

      if !token.Valid { // Token is invalid, maybe not signed correctly
          w.WriteHeader(http.StatusUnauthorized)  // Unauthorized status code
          return // Exit the middleware without calling next handler
      }

        // Token is valid, call next handler
        next.ServeHTTP(w, r)

    })
}
```

6 mistakes and vulnerabilities

https://madappgang.com/blog/chat-gpt-code-errors/

https://cacm.acm.org/blogs/blog-cacm/273577-ai-does-not-help-programmers/fulltext

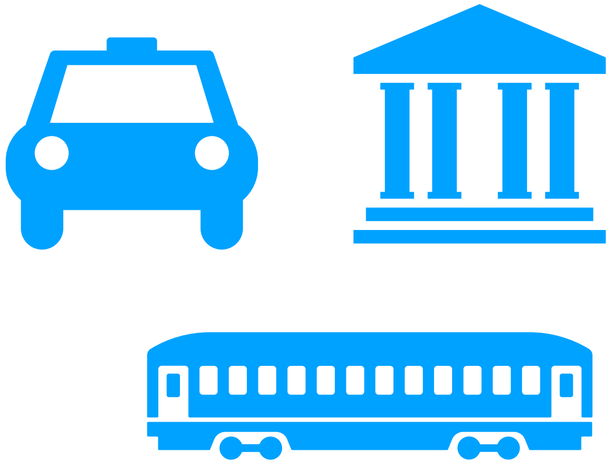
…and All the Things we Discussed Many Times

Interpretability of the Algorithm

Explainability of the Results

Trustworthiness

Reliability



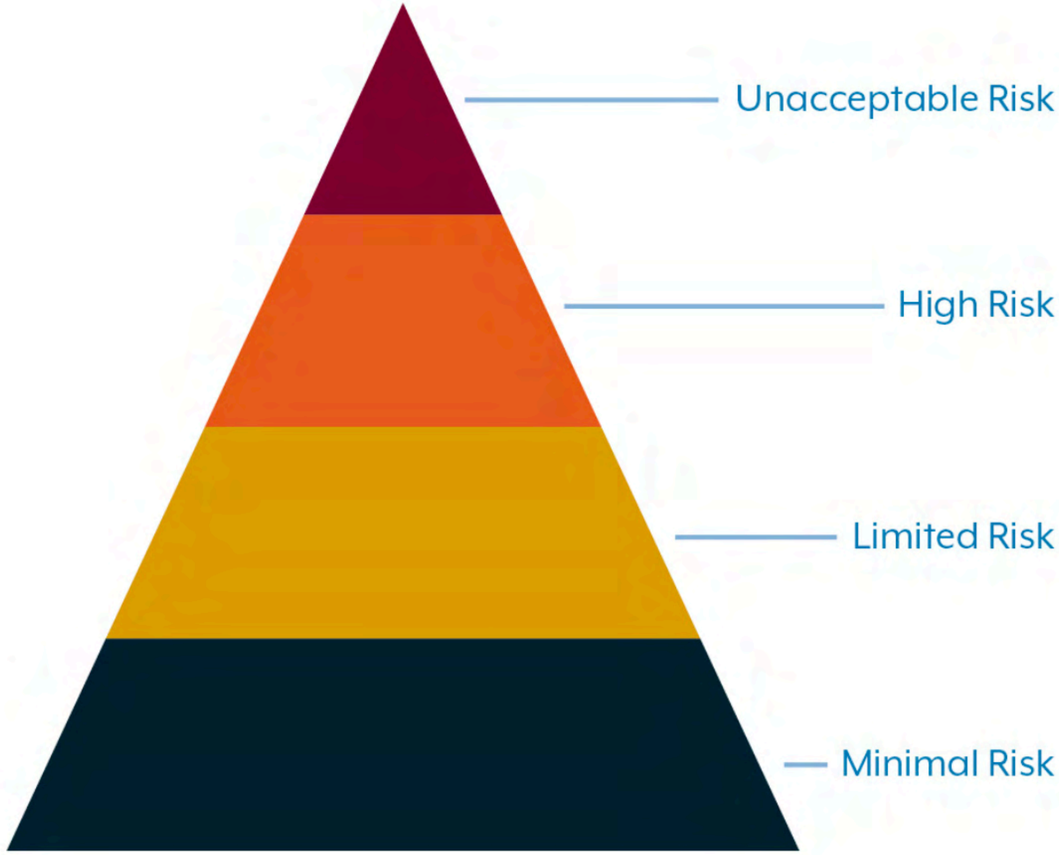
Responsibility of the Decision

Power Consumption

Regulating AI

The European AI Act

Parliament's priority is to make sure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly.



Social scoring systems, people monitoring systems in public spaces (usage is prohibited)

Medical applications, recruitment tools, education, legal advice (mission-critical software process)

Chatbots and deepfakes (it should be clearly stated that you deal with an AI)

Computer games, spam filters, etc. (no regulation)

Risk Perspective

USA and UK

- Less mature developments, no AI act in USA, high-level White Paper in UK

- **USA**, June 12 (Reuters) - U.N. Secretary-General Antonio Guterres on Monday backed a proposal by some artificial intelligence executives for the **creation of an international AI watchdog body like the International Atomic Energy Agency (IAEA)**

Resource Perspective

- **UK, White paper "AI regulation: a pro-innovation approach":** the UK's approach is intended to focus on **promoting innovation and experimentation**, whilst maintaining a **light touch** in terms of regulation.

Innovation Perspective

China

Political perspective

- Well-developed, **several laws** and acts already existed for AI
- Measures for the Management of Generative Artificial Intelligence Services (Draft April 2023, Published July 2023):
  - "Content generated through the use of generative AI shall reflect the Socialist Core Values, and may not contain: **subversion of state power**…"
  - "In the process of algorithm design, training data selection, model generation and optimization, and service provision, take effective measures to **prevent discrimination** based on ethnicity, belief, country, region, gender, age, occupation, health, etc.;"
  - "Respect intellectual **property rights**, business ethics, keep business secrets, and not use algorithms, data, platforms, and other advantages to implement monopoly and unfair competition"
  - "Respect the legitimate **rights and interests of others**, and must not endanger the physical and mental health of others, and must not infringe on the portrait rights, reputation rights, honor rights, privacy rights, and personal information rights of others;"

https://www.china-briefing.com/news/understanding-chinas-new-regulations-on-generative-ai-draft-measures/

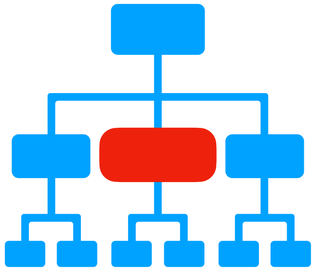
https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023/

https://www.china-briefing.com/news/how-to-interpret-chinas-first-effort-to-regulate-generative-ai-measures/

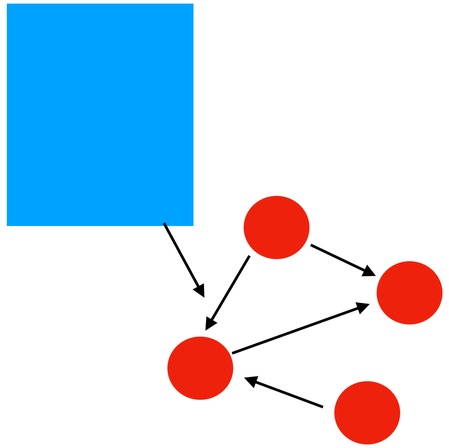
AI (and LLMs) for Requirements Engineering

NLP for RE: a Brief History

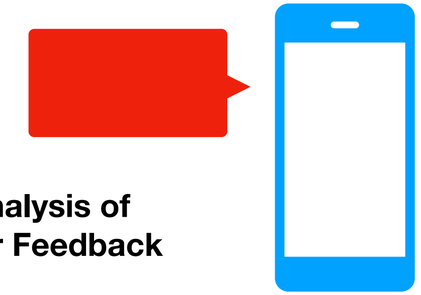
NLP4RE Tasks



Classification

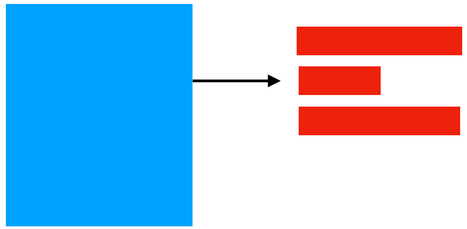


Model Synthesis

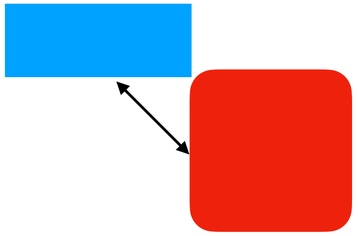


Analysis of
User Feedback

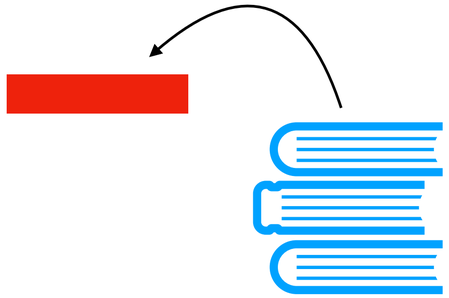
Defect
Detection



Glossary
Extraction



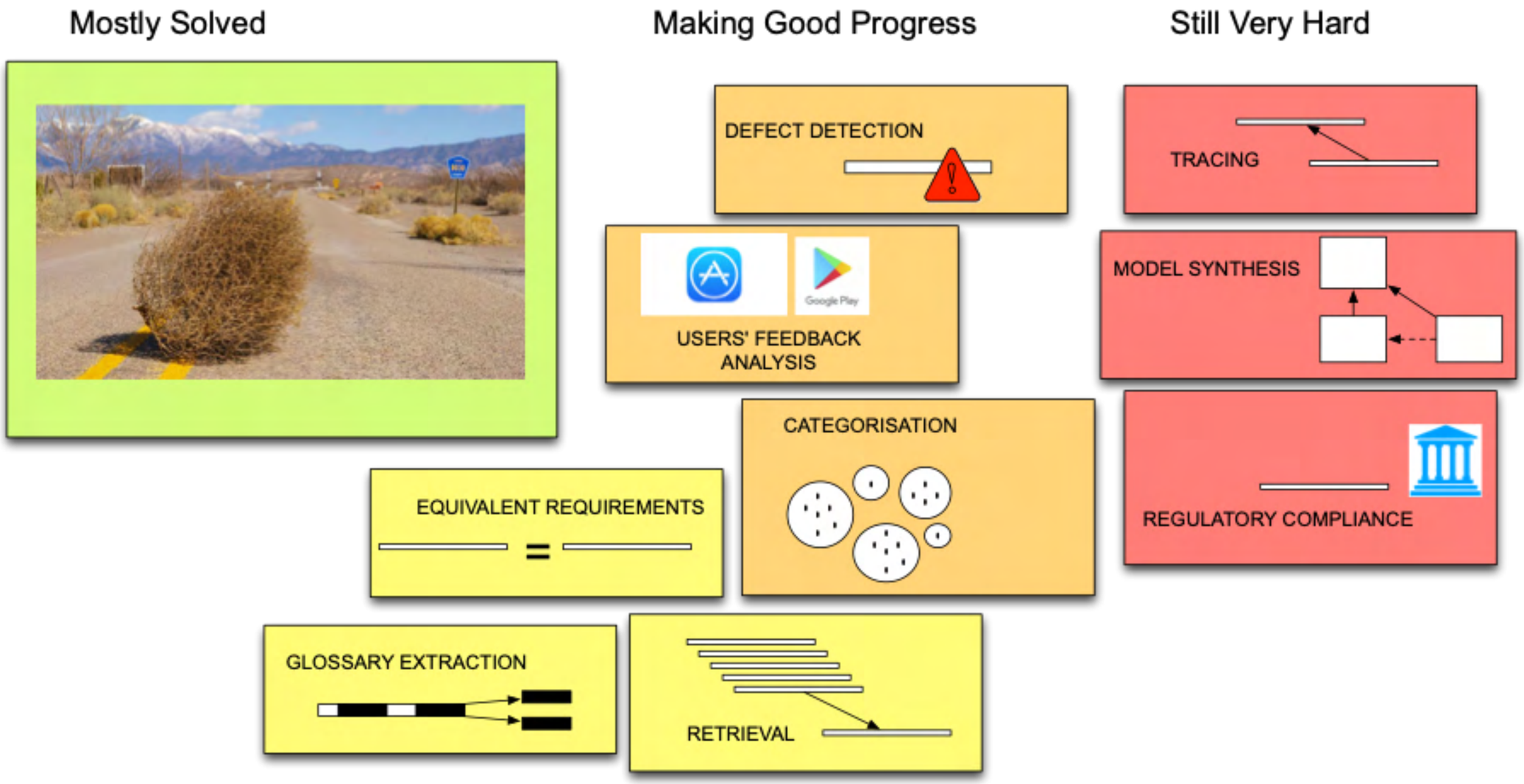
Tracing & Relating



Search & Retrieval

Regulatory
Compliance

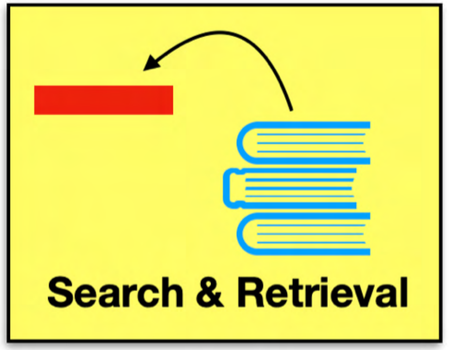
NLP4RE: 2018


Mostly Solved
Making Good Progress
Still Very Hard
DEFECT DETECTION
TRACING
USERS' FEEDBACK ANALYSIS
MODEL SYNTHESIS
CATEGORISATION
EQUIVALENT REQUIREMENTS
REGULATORY COMPLIANCE
GLOSSARY EXTRACTION
RETRIEVAL

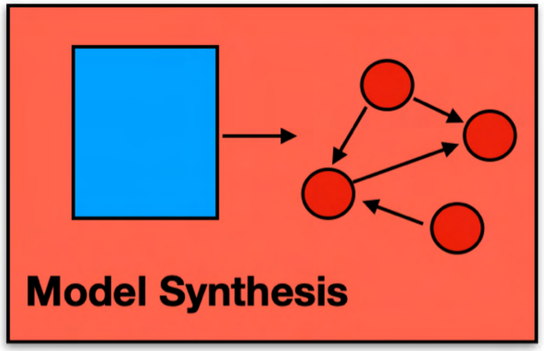
NLP4RE: 2021

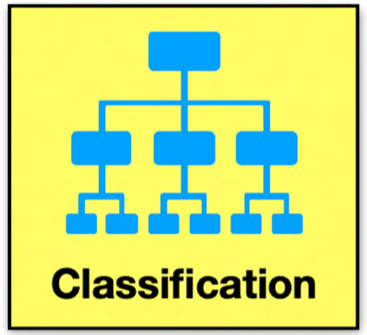
Mostly Solved

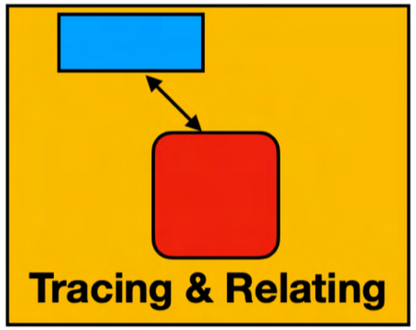
Making Good Progress

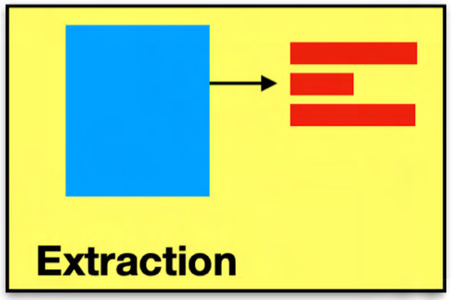


Still Very Hard

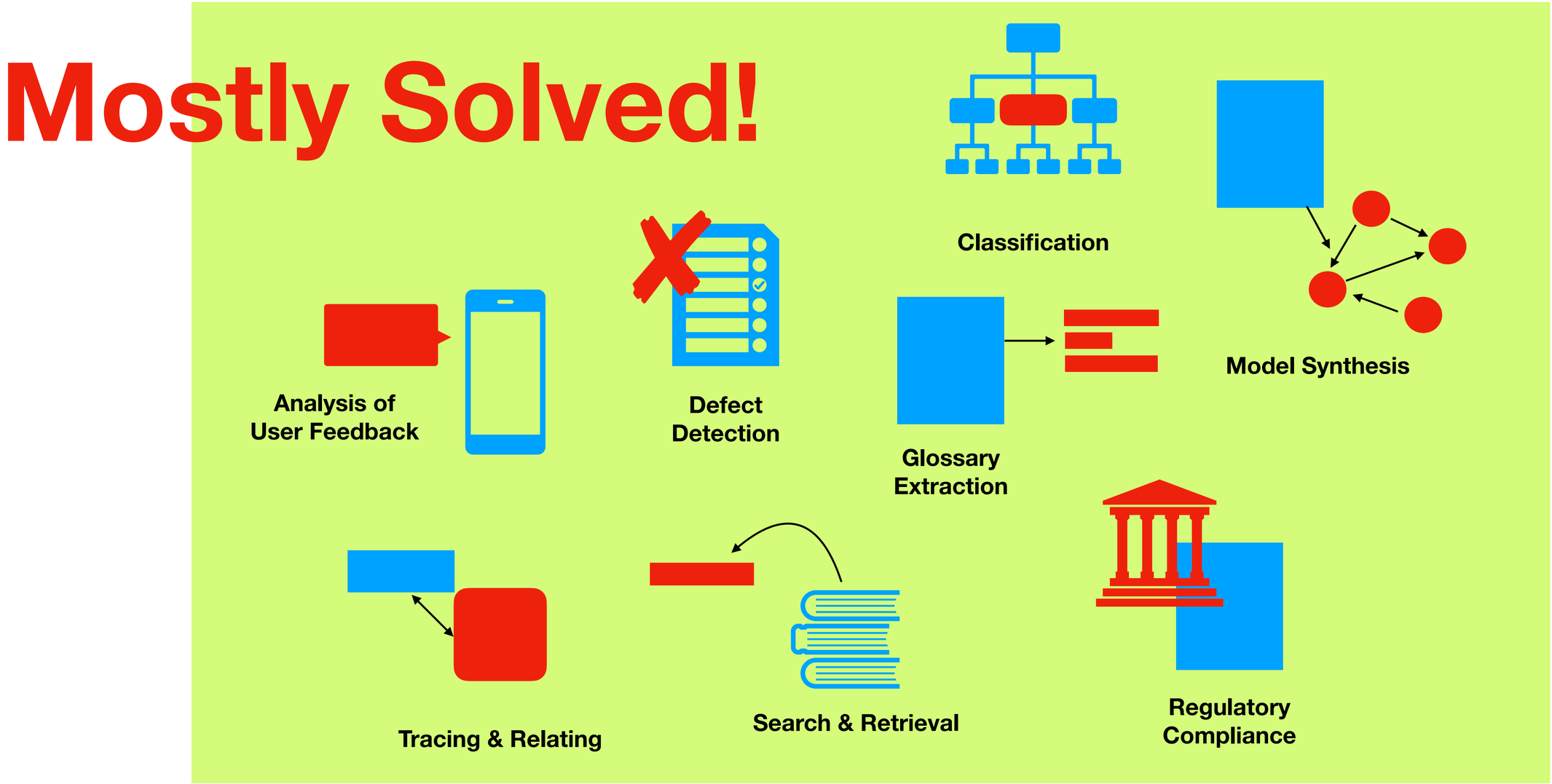








NLP4RE 2023


Mostly Solved!
Classification
Model Synthesis
Analysis of
User Feedback
Defect
Detection
Glossary
Extraction
Tracing & Relating
Search & Retrieval
Regulatory
Compliance

What Can we do TODAY?

Image by pressfoto on Freepi

Classification

a

Please act as a requirements classification tool. What are the possible nonfunctional requirements classes of this requirement? "The authentication system should be and easy to use and prevent access from underage users."

The requirement "The authentication system should be easy to use and prevent access from underage users" can be classified into the following nonfunctional requirements classes:

1. **Usability or User Experience**: This class encompasses the aspect of the requirement that focuses on the system being "easy to use." It pertains to the user's interaction with the authentication system, ensuring that it is intuitive, user-friendly, and minimizes the cognitive effort required for users to successfully authenticate themselves.
2. **Security**: This class covers the aspect of the requirement that emphasizes the system's ability to "prevent access from underage users." It deals with security-related concerns, including access control mechanisms, user authentication processes, and measures to ensure that only authorized users, who meet certain criteria like being of a certain age, can access the system.

Recommendation

a How could you ensure that the system prevents access from underage users?

1. **Age Verification Process**: Implement an age verification process during user registration or account creation. This could involve asking users to provide their date of birth and verifying it against a trusted data source, such as a government-issued identification document.
2. **Identity Verification**: Use identity verification methods to confirm that users are who they claim to be. This could involve requesting additional identification documents or using third-party services that can verify identity.
3. **Parental Consent**: For users who are minors, require parental consent before granting access. This could involve sending notifications or requests to a parent or guardian's email or phone number for confirmation.
4. **Account Approval**: Implement a manual review process for user accounts, especially if age verification is difficult to automate. Human moderators could review accounts and verify the age of users before granting access.
5. **Restrictive Content Filtering**: Implement content filtering mechanisms to restrict access to age-inappropriate content for underage users. This could be particularly important in systems where content is user-generated.
6. **Captcha and Challenge-Response Tests**: Use captchas or challenge-response tests during account creation or login processes to ensure that the user is not a bot or automated script trying to bypass age restrictions.
7. **Two-Factor Authentication (2FA)**: Require users to undergo an additional authentication step, such as receiving a code on their mobile device, to verify their identity and age.

Feedback Analysis

GiutarTuna is an app for guitar tuning and learning

Please consider the GuitarTuna App, and its reviews from users. What are the main concerns of the users? Please associate each concern to a non-functional requirement class

Bing Chat

Here are some of the main concerns of the users and their possible non-functional requirement classes:

Accuracy: Some users complained that the app is not accurate enough for tuning their guitars, especially in noisy environments or with alternate tunings. This could affect the usability and reliability of the app.
Performance: Some users reported that the app is slow to load, crashes frequently, or drains the battery too fast. This could affect the efficiency and availability of the app.
Security: Some users expressed concerns about the app's data collection and privacy policies, especially regarding the microphone access and location tracking. This could affect the confidentiality and integrity of the app.
Compatibility: Some users mentioned that the app is not compatible with their devices, operating systems, or other apps. This could affect the portability and interoperability of the app.
Cost: Some users felt that the app is too expensive for its features, or that the subscription model is not fair or transparent. This could affect the affordability and maintainability of the app.

Creative Requirements Definition

Please act as a creative requirements engineer. Could you please provide a set of user stories for an app that should support guitar tuning, and embed also other social functionalities?

ChatGPT

As a guitarist, I want to use the app to accurately tune my guitar by providing visual indicators and audio feedback, so I can achieve precise tuning for each string.
As a beginner guitarist, I want the app to offer step-by-step instructions and tutorials on guitar tuning, helping me learn and improve my tuning skills.
As a guitarist in a band, I want the app to allow me to save and recall custom tunings for different songs or playing styles, so I can quickly switch between tunings during rehearsals or performances.
As a musician, I want the app to provide a variety of alternate tunings for different genres or playing techniques, allowing me to explore new sounds and experiment with different tunings.
As a guitarist interested in learning new songs, I want the app to provide a library of popular songs with their associated tunings, enabling me to tune my guitar correctly for each song I want to learn.
As a guitarist who enjoys jamming with others, I want the app to include a jam session feature where I can connect with fellow musicians, share recordings, and collaborate on improvisations or song ideas.
As a guitarist seeking feedback and improvement, I want the app to allow me to record and share my guitar playing with a community of fellow musicians, enabling them to provide comments, suggestions, and support.
As a guitarist looking to connect with like-minded musicians, I want the app to include a social network feature where I can discover and connect with other guitarists, join groups, and participate in discussions.
As a guitarist who enjoys challenges, I want the app to offer gamified elements such as daily tuning challenges, achievements, and leaderboards, allowing me to compete and compare my tuning skills with other users.
As a guitarist who wants to stay up-to-date with the latest news and trends in the guitar world, I want the app to provide a curated feed of guitar-related content, including articles, tutorials, gear reviews, and artist interviews.

Ambiguity

a

Please act as an ambiguity detection tool for requirements. Does the following sentence contain any ambiguities? Sentence: The onboard device sends a connection request to the wayside and monitoring subsystem and it responds with an acknowledgment or aborts the connection

The sentence "The onboard device sends a connection request to the wayside and monitoring subsystem and it responds with an acknowledgment or aborts the connection" contains a potential ambiguity:

1. **"It responds with an acknowledgment or aborts the connection"**: The ambiguity here lies in what exactly is meant by "it." Does "it" refer to the onboard device, the wayside and monitoring subsystem, or some other entity? It's unclear which component is responsible for responding with the acknowledgment or abort action.

To clarify this requirement, you might want to specify which entity is responsible for sending the acknowledgment or initiating the connection termination. For example, "The onboard device sends a connection request to the wayside and monitoring subsystem. The subsystem responds with an acknowledgment if successful, or it initiates an abort of the connection request if necessary." This clarification makes it clear which entity is performing each action.

Nocuous anaphora

Ambiguity (cont'd)

a

Please act as an ambiguity detection tool. Is this requirements ambiguous: When the system receives a corrupted message, it terminates the connection with an abort message.

The requirement "When the system receives a corrupted message, it terminates the connection with an abort message" seems relatively clear and straightforward, but there is a minor potential ambiguity that could be clarified:

Innocuous anaphora

1. **"Corrupted message"**: The term "corrupted message" could be interpreted in multiple ways. Does it refer to a message with invalid syntax, a message with incorrect data, or a message that has been tampered with during transmission? Providing a precise definition or clarification of what constitutes a "corrupted message" would help eliminate any ambiguity.

Generality issue

Overall, while the requirement is fairly clear, providing additional details about the nature of a "corrupted message" would enhance its clarity and ensure a common understanding among stakeholders.

Tracing

Please act as a tracing tool, and be very strict with the tracing. By "strict", I intend that only highly related requirements shall be traced to each other. Shall these two requirements be traced to each other? :
1. the onboard system shall have a dashboard.
2. the onboard system shall notify the driver of the maximum speed through an electronic speedometer.

ChatGPT **Yes, these two requirements should be traced to each other.** They are highly related because they belong to the same system and have a common function. The onboard system is responsible for displaying information to the driver and passengers, and one of the information is the maximum speed. **The electronic speedometer is a component of the dashboard that shows the maximum speed to the driver.** Therefore, there is a dependency and a consistency between these two requirements, and they should be traced to each other.

Regulatory Compliance

I have to develop a new health application that allows users to get suggestions from an automated assistant, such as Bing chat or ChatGPT. The application allows users to ask questions and describe their symptoms and the automated assistant will respond with a possible illness and recommendations. Doctors can access the app and confirm the suggestions from the automated assistant. What are the main regulatory requirements that the app shall satisfy? The app will operate in Europe.

Bing Chat

There are different regulatory requirements that the app shall satisfy depending on the type, function, and impact of the app. Based on the description, the app could be considered as a **digital health technology** (DHT) that uses artificial intelligence (AI) to provide suggestions to users and doctors[1]. Some of the main regulatory requirements that the app shall satisfy are:

- **Data protection and privacy**: The app shall comply with the General Data Protection Regulation (GDPR) and other relevant laws that protect the personal data and privacy of users and doctors. The app shall inform users and doctors about what data is collected, how it is used, and how it is shared. The app shall also obtain consent from users and doctors before collecting or processing their data. The app shall also implement appropriate technical and organizational measures to ensure the security and confidentiality of the data[2][1].
- **Safety and performance**: The app shall comply with the Medical Device Regulation (MDR) and other relevant laws that ensure the safety and performance of medical devices. The app shall demonstrate that it is safe, effective, and reliable for its intended purpose. The app shall also undergo a conformity assessment by a notified body to verify its compliance with the MDR. The app shall also be registered in the European Database on Medical Devices (EUDAMED) and bear a CE marking[1][3].
- **Health technology assessment**: The app shall comply with the Regulation on Health Technology Assessment (HTAR) and other relevant laws that evaluate the clinical, economic, social, and ethical impacts of health technologies. The app shall provide evidence on its clinical benefits, risks, costs, and added value compared to existing alternatives. The app shall also cooperate with national authorities and stakeholders to facilitate the adoption and reimbursement of the app in different healthcare systems

Riferimenti:

1. sciencedirect.com
2. digital.health
3. health.ec.europa.eu

Regulatory Compliance (cont'd)

More specifically, which requirements from GDPR?

Bing Chat

- **Lawful basis for processing**: The app shall identify and document a valid lawful basis for processing the personal data of users and doctors, such as consent, contract, legal obligation, vital interest, public interest, or legitimate interest. The app shall also inform users and doctors about the lawful basis and its implications[1][2].
- **Data minimization and purpose limitation**: The app shall only collect and process the personal data that is necessary and relevant for the specific and explicit purpose of providing suggestions to users and doctors. The app shall not use the personal data for other purposes that are incompatible with the original purpose, unless it obtains a new consent or has another lawful basis[1][2].
- **Data quality and accuracy**: The app shall ensure that the personal data it collects and processes is accurate, complete, and up to date. The app shall also provide users and doctors with the means to access, rectify, or erase their personal data if it is inaccurate, incomplete, or outdated[1][2].
- **Data retention and deletion**: The app shall only retain the personal data for as long as it is necessary for the purpose of providing suggestions to users and doctors. The app shall also delete the personal data when it is no longer needed, or when users and doctors request its deletion, unless there is a legal obligation or a legitimate interest to keep it[1][2].
- **Data security and confidentiality**: The app shall implement appropriate technical and organizational measures to protect the personal data from unauthorized or unlawful access, use, disclosure, alteration, or destruction. The app shall also ensure that only authorized persons have access to the personal data on a need-to-know basis. The app shall also report any data breach to the relevant supervisory authority and to the affected users and doctors without undue delay[1][2][4].
- **Data protection by design and by default**: The app shall integrate data protection principles and measures into every stage of its development and operation. The app shall also ensure that the default settings of the app are privacy-friendly and respect the choices of users and doctors[1][2].

…

Completeness

I have the following requirements for a railway system in relation to red signal crossing permission.

Are the requirements that I provided sufficiently complete to make sense of the system behaviour?

Please considere incompleteness both at the requirement level (incompleteness of a single requirement) and incompleteness of the requirements set (in case requirements are missing).

The requirements are:
1. When the driver encounters a red signal, shall stop.
2. After the driver stops, the driver can either wait for a green signal or press the Red Crossing button and perform the Red Crossing Procedure.
3. If the driver decides to perform the Red Crossing procedure, it first need to receive an authorisation from the infrastructure manager.
4. Then, after the authorisation, the driver can press the Red Crossing button for at least 5 seconds and less than 10 seconds.
5. After 5 seconds, a light blinks on the panel.
6. When the light blinks the driver can perform the red crossing.
7. The driver shall perform the red crossing within 30 seconds after the light blinks.
8. If this the red signal is not crossed within the 30 seconds, the onboard system shall automatically stop the train.
9. After 30 seconds from the moment in which it was lighted on, the light stops blinking.

ChatGPT

The requirements that you provided are **not sufficiently complete to make sense of the system behavior.** There are some gaps and ambiguities that need to be clarified and resolved. Here are some ways to modify the requirements to complete them:

- At the requirement level, you should specify the conditions and actions more clearly and consistently. For example, **in requirement 2, you should state what happens if the driver does not press the red crossing button or does not perform the red crossing procedure.** In requirement 4, you should state what happens if the driver presses the red crossing button **for less than 5 seconds or more than 10 seconds.** In requirement 6, you should state how the driver performs the red crossing (e.g., by pressing a pedal or a lever).

- At the requirements set level, you should add some requirements that are missing or implied by the existing ones. For example, you should state what is the purpose and scope of the system, what are the roles and responsibilities of the driver and the infrastructure manager, what are the assumptions and constraints of the system, what are the expected outcomes and quality attributes of the system, and what are the exceptions and error handling mechanisms of the system.

Completeness (cont'd)

Could you please rewrite the requirements in a way that they are complete and internally consistent?

Architectural Requirements

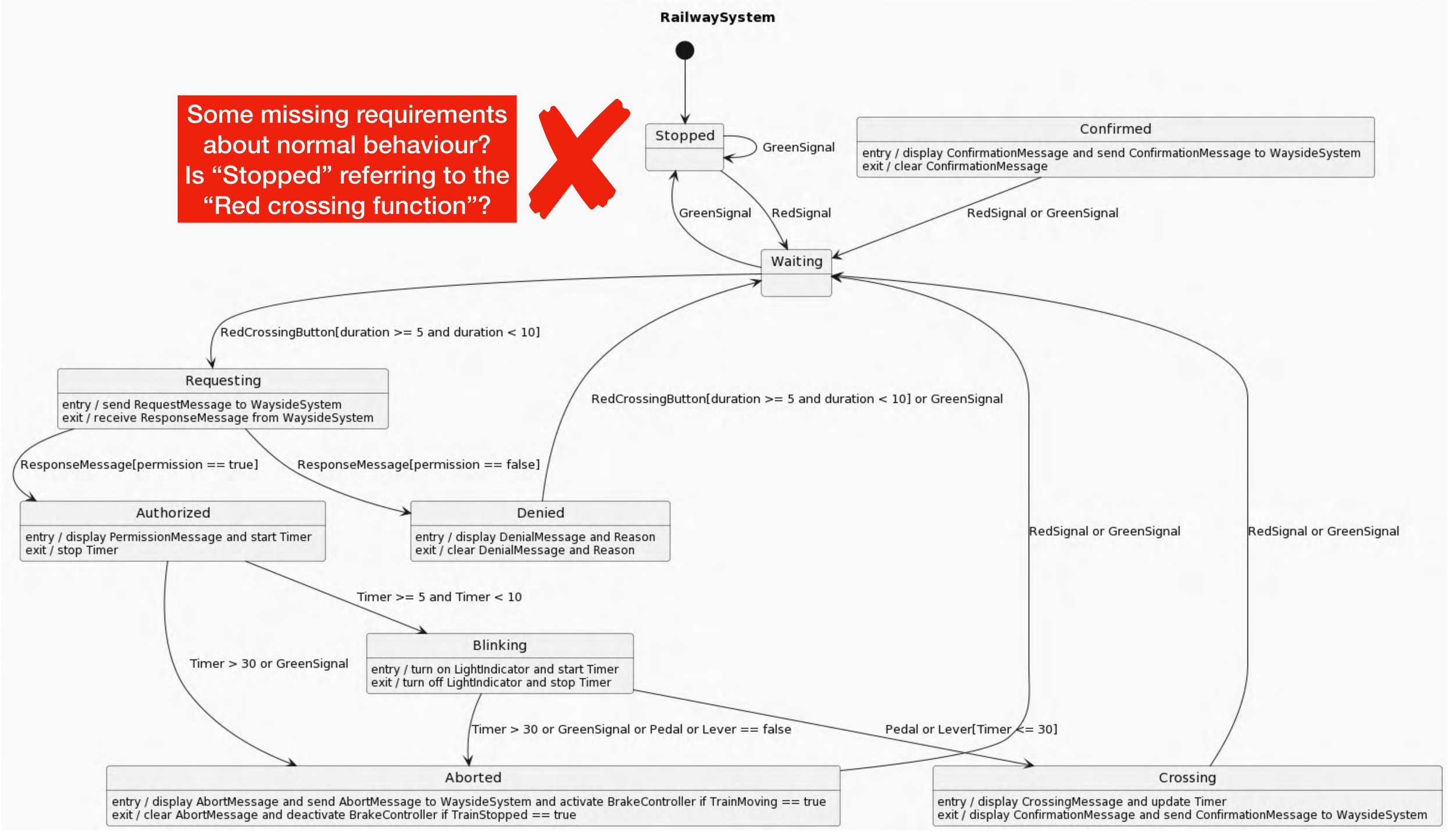
- The system shall provide a **red signal crossing permission function** for the driver of the train when the train encounters a red signal on the railway track.
- The system shall consist of **an onboard system and a wayside system** that communicate with each other via wireless signals.
- The onboard system shall consist of a dashboard, a red crossing button, a light indicator, and a brake controller.
- The wayside system shall consist of a signal controller, a track circuit, and an infrastructure manager station.

Standard Behaviour

- When the train encounters a red signal, the onboard system shall display a red signal icon on the dashboard and the driver shall stop the train before the signal.
- **After the driver stops the train, the driver can either wait for a green signal or request a red crossing permission from the infrastructure manager by pressing and holding the red crossing button for at least 5 seconds and less than 10 seconds.**
- If the driver presses and holds the red crossing button for less than 5 seconds or more than 10 seconds, the onboard system shall display an error message on the dashboard and ignore the request.
- If the driver presses and holds the red crossing button for at least 5 seconds and less than 10 seconds, the onboard system shall send a request message to the wayside system and display a waiting message on the dashboard.

Other perspectives

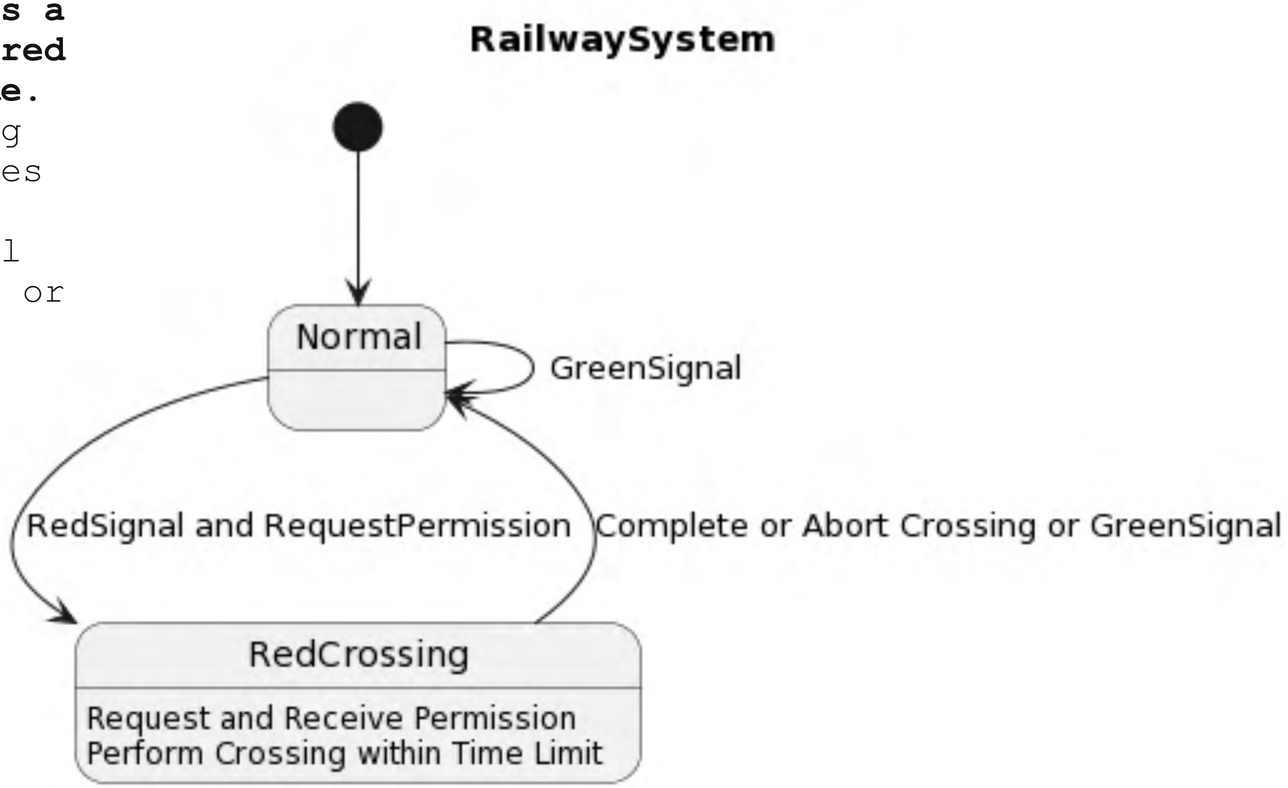
- The wayside system shall receive the request message from the onboard system and forward it to the infrastructure manager station.
- **The infrastructure manager shall review the request message and decide whether to grant or deny the red crossing permission based on the safety and operational conditions of the railway track.**
- The infrastructure manager shall send a response message to the wayside system indicating the decision and the reason.


RailwaySystem
Some missing requirements about normal behaviour? Is “Stopped” referring to the “Red crossing function”?
Stopped
GreenSignal
Confirmed
entry / display ConfirmationMessage and send ConfirmationMessage to WaysideSystem
exit / clear ConfirmationMessage
GreenSignal
RedSignal
RedSignal or GreenSignal
Waiting
RedCrossingButton[duration >= 5 and duration < 10]
Requesting
entry / send RequestMessage to WaysideSystem
exit / receive ResponseMessage from WaysideSystem
RedCrossingButton[duration >= 5 and duration < 10] or GreenSignal
ResponseMessage[permission == true]
ResponseMessage[permission == false]
Authorized
entry / display PermissionMessage and start Timer
exit / stop Timer
Denied
entry / display DenialMessage and Reason
exit / clear DenialMessage and Reason
RedSignal or GreenSignal
RedSignal or GreenSignal
Timer >= 5 and Timer < 10
Blinking
entry / turn on LightIndicator and start Timer
exit / turn off LightIndicator and stop Timer
Timer > 30 or GreenSignal
Timer > 30 or GreenSignal or Pedal or Lever == false
Pedal or Lever[Timer <= 30]
Aborted
entry / display AbortMessage and send AbortMessage to WaysideSystem and activate BrakeController if TrainMoving == true
exit / clear AbortMessage and deactivate BrakeController if TrainStopped == true
Crossing
entry / display CrossingMessage and update Timer
exit / display ConfirmationMessage and send ConfirmationMessage to WaysideSystem

Abstraction

Could you provide a more high-level description of the behaviour, and provide this abstract representation in PlantUML?

- The system has two **main modes:** Normal and RedCrossing.
- In Normal mode, the system follows the signals from the wayside system and stops or resumes the train accordingly.
- In **RedCrossing mode, the system requests and receives a permission from the infrastructure manager to cross a red signal, and performs the crossing within a limited time.**
- The system can switch from Normal mode to RedCrossing mode when the driver encounters a red signal and decides to request a permission.
- The system can switch from RedCrossing mode to Normal mode when the driver completes or aborts the crossing, or encounters a green signal.



Is REALLY Everything Solved? Survival Strategies for Depressed RE Researchers

[Submitted on 31 Mar 2023]

Choose Your Weapon: Survival Strategies for Depressed AI Academics

Julian Togelius, Georgios N. Yannakakis

The Job(s) of Requirements Engineers

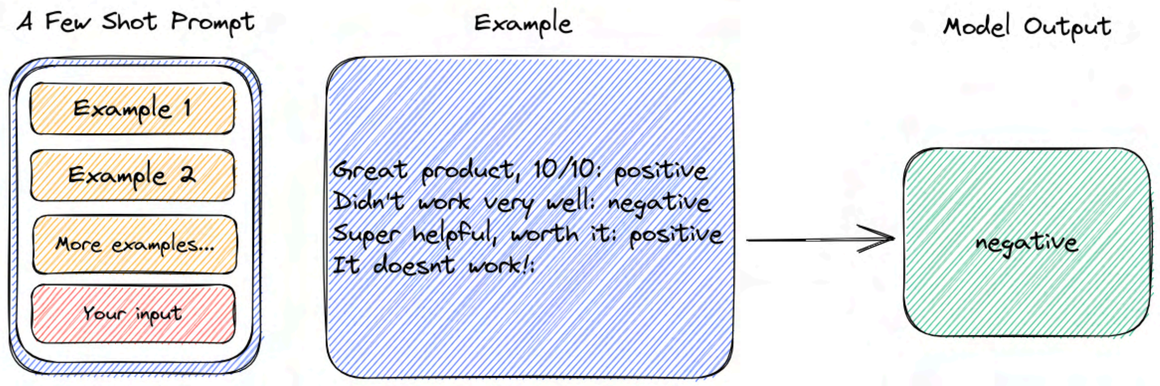
Image by Freepik

(AI for RE) Prompt Engineering

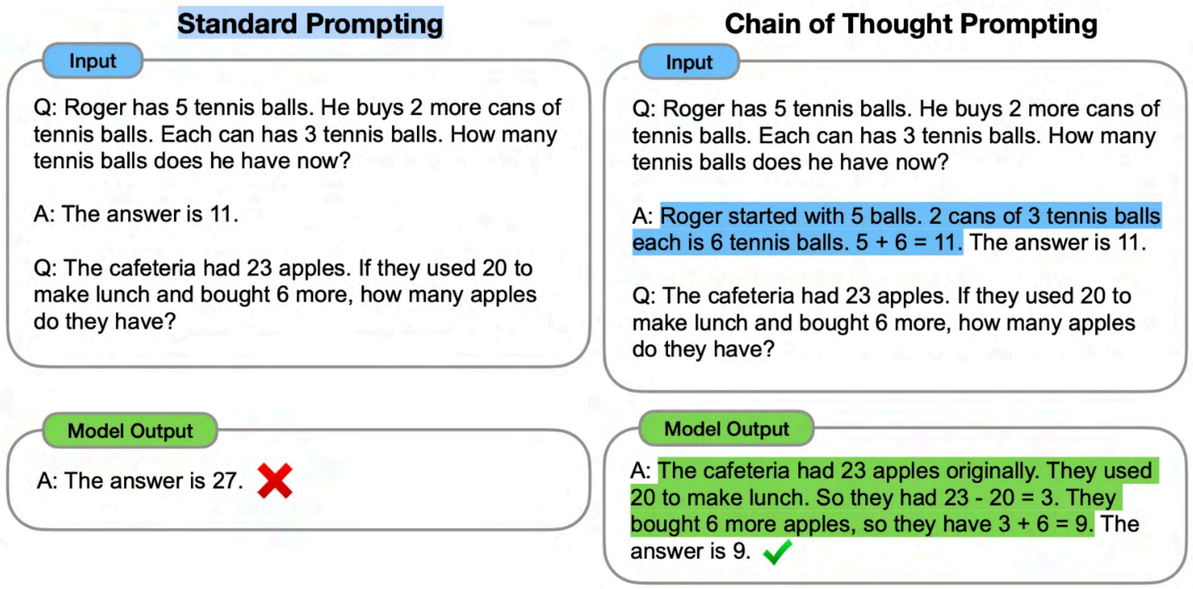
Prompting is the new requirements definition

When I specify a prompt to produce an UML diagram or some program, I am actually specifying requirements to satisfy

We need to provide strategies for prompting towards software development



Few-shot Prompting



Chain of Thought Prompting

…and tune temperature and other parameters

Our experience in writing high-quality requirements can help in the next future of software engineering

(AI for RE) Address More Complex Tasks

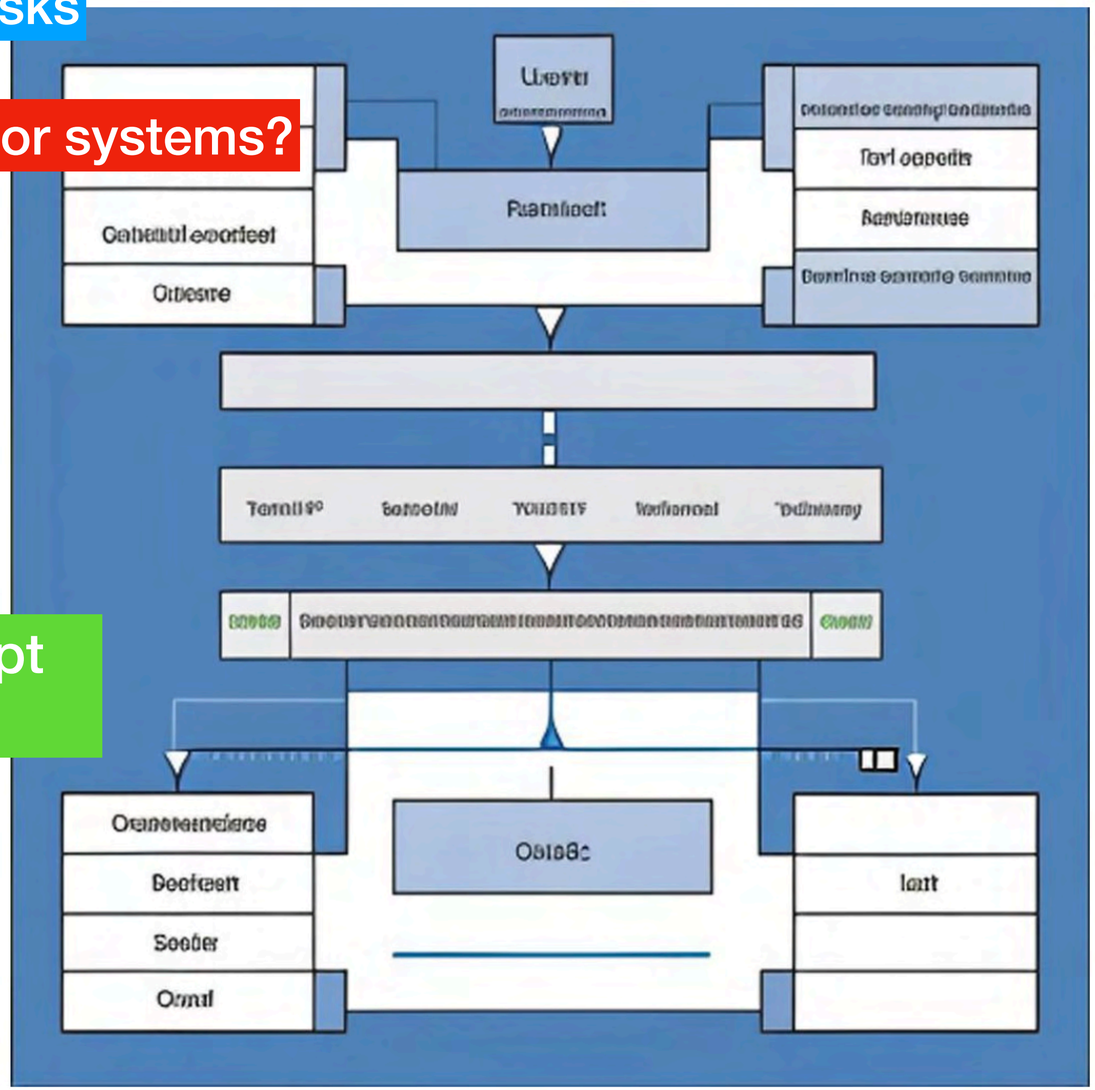
ChatGPT and similar can list actions to solve simple tasks

How to connect prompts to build entire programs or systems?

How do we connect with legacy systems?

How to create a goal-oriented chain of prompts?

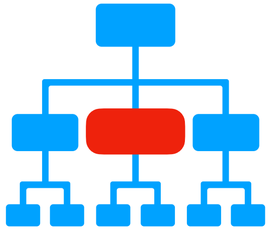
Software engineering becomes high-level prompt engineering (aka requirements engineering)



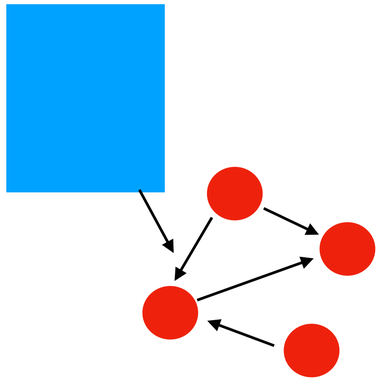
Checkout also MetaGPT: https://github.com/geekan/MetaGPT

(AI for RE) Exploit Potential of LLMs for RE

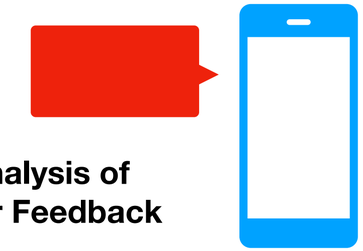
NLP4RE Tasks



Classification

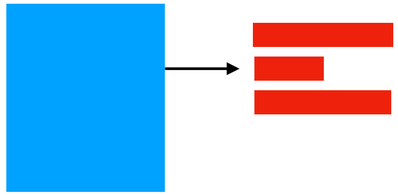


Model Synthesis

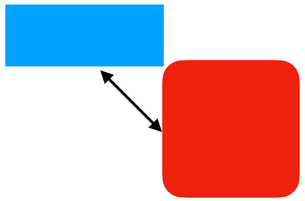


Analysis of User Feedback

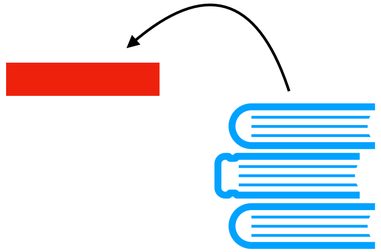
Defect Detection



Glossary Extraction



Tracing & Relating



Search & Retrieval

Regulatory Compliance

Prompting strategies are needed for each task

DO USER STUDIES!

(AI for RE)…and Business as Usual

Requirements are often confidential and need to be internally processed by companies (so no LLMs as-a-service)

Small LLMs that run on a machine can be sufficient for the analysis of requirements

Simple solutions are often sufficient and better explainable (we need to rely on the output of our ML systems)

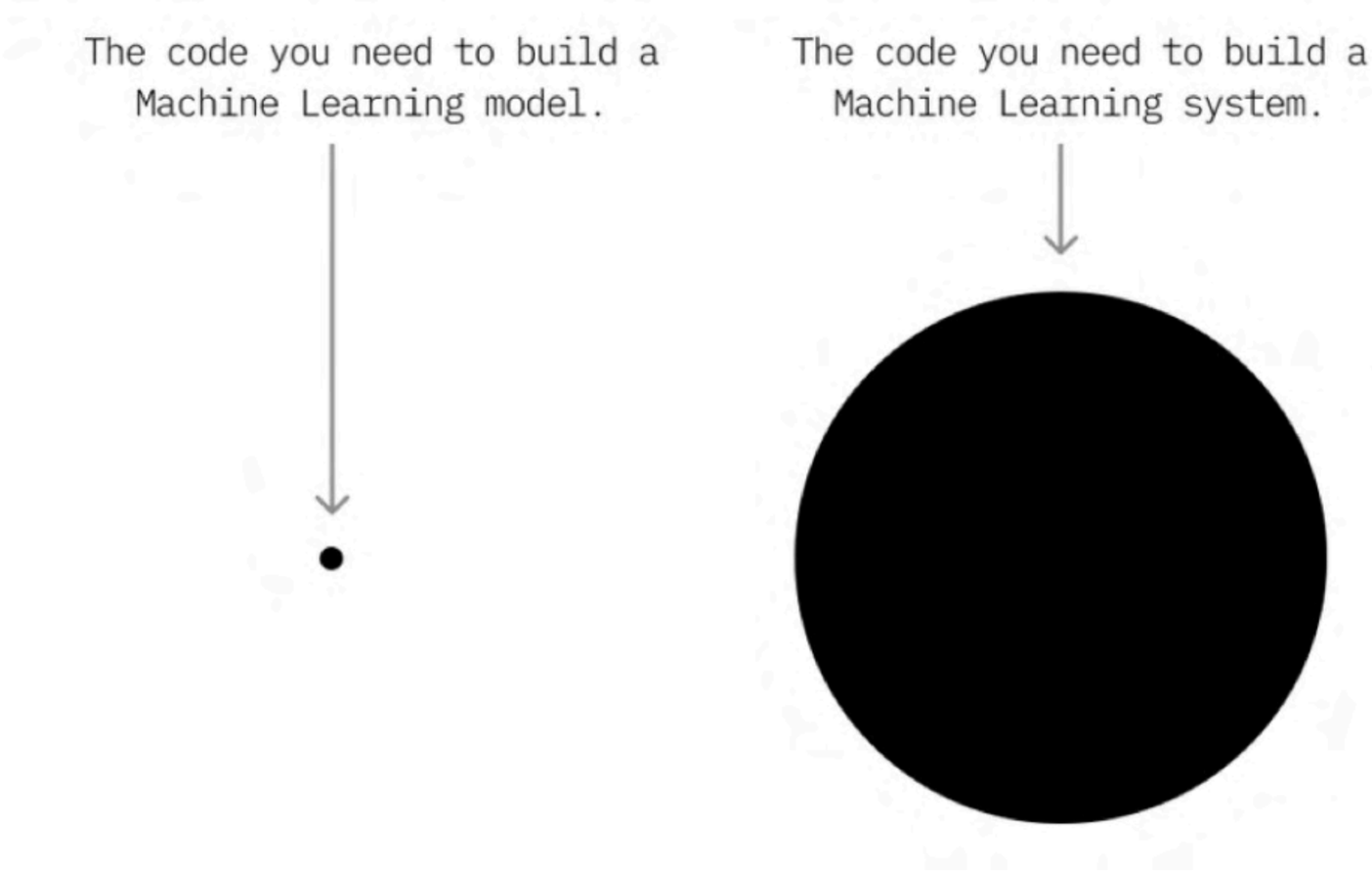
Proprietary LLMs become the benchmark for performance

LLMs can be used to ANNOTATE data

(RE for AI) Address RE Issues in AI-intensive Systems

Explainability, Interpretability, Accountability, Trustworthiness, Power Consumption…

Credits: @svpino



Consider AI in-context

Several studies on RE issues of AI systems

More studies on SOLUTIONS (although solution papers are more likely to be rejected)

Don’t forget domain-specificity of the solutions (there are many domains besides automotive)

Don’t try to solve all issues at once

(RE for AI) Contribute to Design Dependable AI Systems

AI can improve mission-critical systems (transport, health, public administration)

More efficient transportation, better health, improved administrative efficiency…

These systems need to be DEPENDABLE (safe, secure, available, reliable, maintainable)

The problem is not different from cyber-physical safety critical systems
(nature and electronics are not fully predictable)

REDUNDANCY and DIVERSITY are the key solutions

Diversity in AI code, in NN architectures, in datasets, in testing, etc.

Fear WRONG AI more than EVIL AI!

(RE for AI) Engineer Data Collection

AI is data hungry and we must move from SYSTEM requirements to DATA requirements

What are the relevant entities? How are they related? What is an efficient way of collecting them?

Linguistic and image data has been the focus so far

These data are “easy to collect” and already digitalised

There are many other types of data that are expensive to collect

To get soil-related data you need to go in the field, rent a digger, escavate, sleep, perform lab analysis, etc.

To get ground-truth data about the vegetation, you need to go there, check GPS position, annotate the type of tree, etc. (aerial pictures are not enough)

To perform predictive maintenance of a railway system you need to develop a logging software, load it on a train, connect sensors, etc.

As usual, domain knowledge is critical

(RE for AI) Contribute to Operationalise the AI Act

The AI act is quite general and technology providers do not have a guideline to put it into practice

We should contribute to give more detailed practical guidelines

Guidelines shall be domain-specific as for other regulations (CENELEC, DO178B, 93/42/EEC)

Regulations shall also be directed towards the market

AI is in the hands of an oligopoly of large companies

Find strategies to bring public academia and open source at the center of AI developments

As many problems have a societal impact, we need to connect with policymakers

Prevent OVERREGULATION!

Stay One Step Ahead

We need to look forward and consider issues that could manifest themselves in the future

- **Multimodality and Embodiment:** intelligence raises from interaction with the world and multimodality (**Palm-E** is already there…https://palm-e.github.io/), what are the consequences of AI robots in society?

- **Artificial General Intelligence (AGI) and alignment:** how can we ensure that an AGI responds to human values? How to precisely describe and measure values? Is this even desirable (humanity has many negative values…)?

- **Artificial Superintelligence (ASI):** what would be our place in a world with systems that are smarter than us (and connected)? Will there be an existential risk? How much power are we already handing to AI? Will ASI be power-seeking?

- **Consciousness:** what will happen when these AI will become conscious (and how will we establish that)?

- **Open source:** if AI is such as an atomic bomb, why making atomic bombs open source?

Questions?