AI.BAY 2023 - Bavarian International Conference on AI

AI as a (safe) Tool for Software Development?

When we talk about AI today, it is often about:

- AI as a driver assistance system (NVIDIA DRIVE, TESLA Autopilot)
- AI for controlling robots (Deep Reinforcement Learning)
- AI for creating images (Stable Diffusion, Dall-E)
- AI for recognizing disease patterns or guiding surgeons

➔ AI is here the product at the end of the development chain

One aspect of AI is considered much less frequently, but has recently celebrated major breakthroughs:

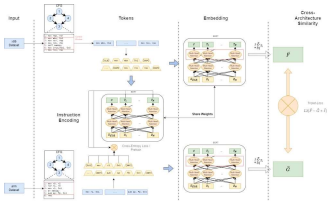
➔ AI as a tool for creating products ←

This is of great importance for development in industry

What are the opportunities and risks of the two directions?

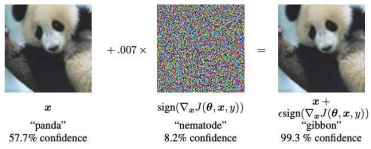
Opportunities

Feng, D. et al. Deep multi-modal object detection and semantic segmentation for autonomous driving: Datasets, methods, and challenges. IEEE ITS (2020)



Bayerl, D. et al. AutoBERT: A Deep Bidirectional Transformer for Cross-Architecture Binary Function Embeddings. (2023)

Risks



Goodfellow et al. Explaining and Harnessing Adversarial Examples. ICLR (2015)

„write a function in python that signs a given message using a ecdsa signing key"

```
def sign_message(message):
    private_key = binascii.unhexlify("e331b6d69882b4cb4ea581d88 ...
    [...]
```

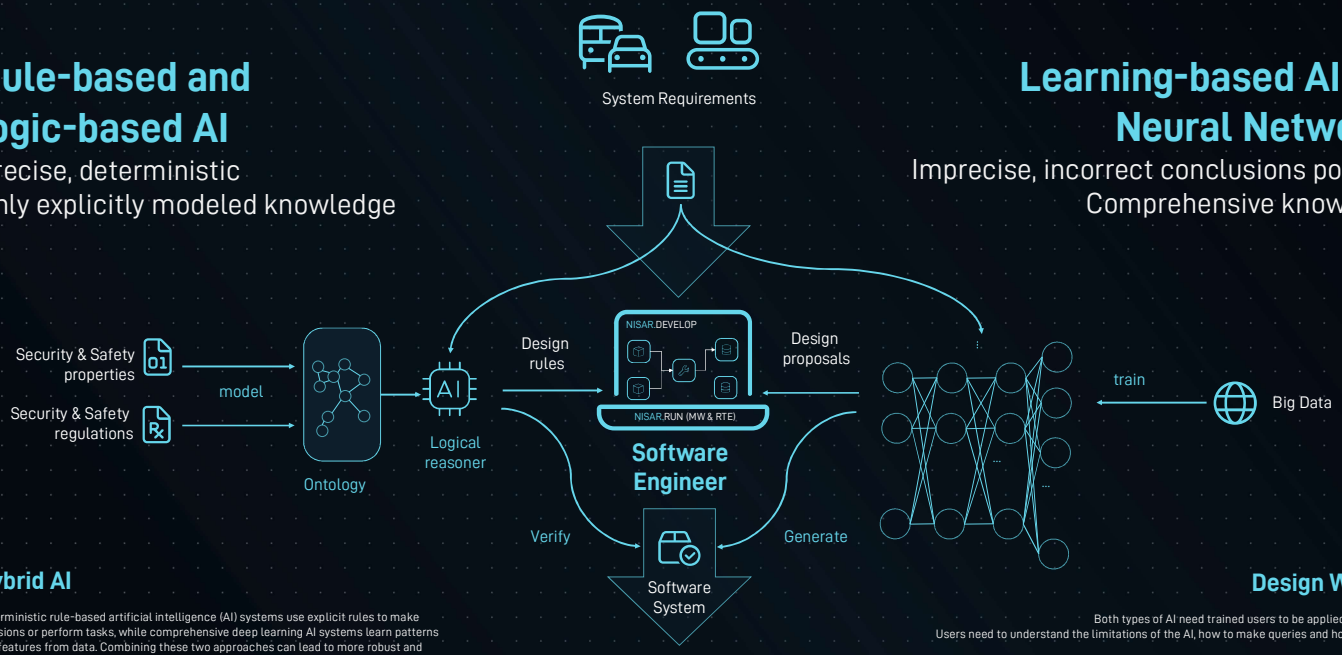
Perry, N. et al. Do Users Write More Insecure Code with AI Assistants? (2022)

Rule-based and logic-based AI

Precise, deterministic
Only explicitly modeled knowledge

Learning-based AI and Neural Networks

Imprecise, incorrect conclusions possible
Comprehensive knowledge



Hybrid AI

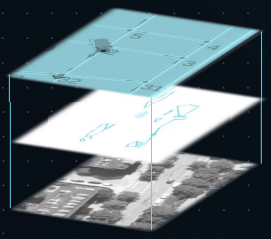
Deterministic rule-based artificial intelligence (AI) systems use explicit rules to make decisions or perform tasks, while comprehensive deep learning AI systems learn patterns and features from data. Combining these two approaches can lead to more robust and reliable AI systems.

One approach to combining these two types of AI is to use a hybrid system, where a deterministic rule-based system provides high-level guidance or constraints to a deep learning system. For example, a rule-based system could be used to determine the initial direction of a self-driving car, while a deep learning system could be used to make finer adjustments based on real-time sensor data.

Another approach is to use deep learning to improve the performance of rule-based systems by automating the process of rule generation or tuning. For example, a deep learning system could analyze large amounts of data to identify patterns and rules that a human expert may have missed, or it could learn to optimize the parameters of a rule-based system based on performance feedback.

Overall, combining deterministic rule-based AI and comprehensive deep learning AI can lead to more powerful and versatile AI systems, with the potential to improve performance and reliability in a wide range of applications.

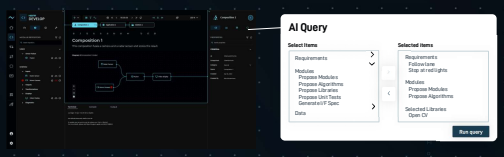
Open AI Chat-GPT3, as of 17.02.2023



Design Wizards

Both types of AI need trained users to be applied successfully
Users need to understand the limitations of the AI, how to make queries and how to evaluate the results.

In order to bring AI to it's full potential as a tool, the AI has to be encapsulated by a logic to reduce the complexity for the user. This logic can be an AI by its' own right.
This logic has to implement the engineering flows and processes of the relevant domain. Particularly, approaches of gradual refinement have to be hidden to ensure an efficient workflow.



M.Sc. Dominik Bayerl

CARISSMA

Center of Automotive Research on Integrated Safety Systems and Measurement Area
Technische Hochschule Ingolstadt
Esplanade 10, 85049 Ingolstadt

Dr.-Ing. Michael Göller

NISAR
We simplify software development

NISAR Autonomy GmbH
Garching Forschungszentrum
Lichtenbergstraße 8, 85748 Garching b. München
m.goeller@nisar.ai