Human-AI Engineering for Adults

André MEYER-VITALI a,1, and Wico MULDER b

aDFKI, Saarbrücken
bTNO, Groningen

ORCiD ID: André Meyer-Vitali https://orcid.org/0000-0002-5242-1443, Wico Mulder https://orcid.org/0000-0002-8607-0055

Abstract. The engineering of reliable and trustworthy AI systems needs to mature. While facing unprecedented challenges, there is much to be learned from other engineering disciplines. We focus on the five pillars of (i) Models & Explanations, (ii) Causality & Grounding, (iii) Modularity & Compositionality, (iv) Human Agency & Oversight, and (v) Maturity Models. Based on these pillars, a new AI engineering discipline might emerge, which we aim to support using corresponding methods and tools for ‘Trust by Design’. A use case concerning mobility and energy consumption in an urban context is discussed.

Keywords. Software Engineering, Artificial Intelligence, Models, Modules, Trust, Causality, Robustness, Explainability, Agency, Multi-Agent Systems, Smart Cities, Human-Computer Interaction, Context-Aware Pervasive Systems, Maturity Model

1. Introduction

The current wave of Artificial Intelligence (AI) is characterised by Deep Learning [1, 2], Transformers [3, 4] and Large Foundation Models [5]. Whilst the impact of such systems touches almost all veins of our society, it seems that we are reaching the limits of controlled engineering of these large, highly interconnected, AI-based systems.

On the one hand, we see their complexity increase on an individual level, as well as on their connected dependency levels, whilst on the other hand, we see a growing lack of experience on the level of their design and engineering. The complexity of existing AI models is often beyond our understanding, and the methods and processes to ensure safety, reliability, and transparency are lacking. This poses serious risks at the level of trustworthiness, particularly when it comes to critical applications with significant physical, economic, or social impact. The AI systems used in such applications are required – for example by the European AI Act – to have been thoroughly designed, validated and certified according to well-defined criteria.

Recent developments in Generative AI are based on so-called ‘Foundation Models’, which can appear as Large Language Models (LLM) or as similar multi-modal models of still images, videos and others. The transformer architectures that generate these
models convert huge amounts of text or other media content into statistical models of co-occurrence of tokens (parts of words or other features).

Many are not aware that deep learning does not support a real understanding of problems. At a first glance, these models for generative AI seem to understand human language and creative expression. However, as they are uniquely based on producing probabilistic assemblies of tokens, they do not even understand language itself. There is no grammar involved or any form of semantics. They only reflect high-dimensional statistical correlations.

Great disillusionment set in as problems, such as insufficient internal representation of meaning (interpretability and transparency), susceptibility to changes in the input signal (robustness), lack of transferability to cases not covered by the data (generalisation) and, last but not least, the thirst for big data and processing itself (efficiency, adequacy, sustainability), became apparent. Some of these problems are a direct result of the massive use of deep learning black-box methods that depend solely on data [6].

To increase the grip and understanding of the outcomes of large neural models, new approaches combine data-oriented machine learning with symbolic conclusions and the explicit representation of knowledge [7, 8].

Such types of approaches are being advanced by the term ‘Trusted AI’. Trusted AI aims to create a new generation of AI systems that guarantee functionality, allowing use even in critical applications [9]. Developers, domain experts, users, and regulators can rely on performance and reliability even for complex socio-technical systems. Trusted AI is characterised by a high degree of robustness, transparency, fairness, and verifiability, where the functionality of existing systems is in no way compromised, but actually enhanced.

Foundation models are not trustworthy, because they lack any kind of understanding of truth, facts, time, space, concepts, reasons, causes and effects. As they are not consistent, transparent, robust and reliable, it is very risky to trust them in critical applications. Even when they seem to give reasonable answers from time to time, it is impossible to predict when they will fail and start to hallucinate.

We need to stop reinventing the wheel; learning from scratch, but understanding nothing. Instead, we need to use existing knowledge, build on experiments and experience, formulate and validate new hypotheses and theories, in order to gain knowledge and insight at a higher level, and to explain why events happen, predictions are made and decisions or actions are taken. This requires a reinforced attention for engineering processes with an aim to improve scientific progress where one can stand on the shoulders of giants.

This paper therefore sets out five pillars of AI Engineering. Together, they form a supportive framework that fosters ‘Trusted AI by Design’. Section 2 discusses the five pillars and section 3 provides a use case in a smart city context.

2. Trusted AI Engineering

There is a dilemma to overcome in building trustworthy AI systems [10, 11, 9]: on the one hand, we expect AI systems to decide autonomously and intelligently on our behalf, which requires agency and delegation; on the other hand, we require them to be predictable, verifiable, safe and accountable. Of course, there are limits to achieving all
these goals and to guarantee correctness under all circumstances and domains. Instead, there is a trade-off to be made between entirely predictable and correct versus plausible and adaptive behaviour. What matters most is that expectations are managed to create validated trust through experience, shared causal models and theory of mind. Therefore, mutual awareness of assumptions, intentions, expectations and capabilities are required to create a dialogue of trust in human-agent collaboration.

A fundamental difference between traditional software and AI systems is that the outcomes are not necessarily deterministic, but probabilistic, and that there may be more than one "correct answer". Hence, the goal is shifting from guarantees of correctness towards verifying for plausibility. In the section below we discuss the five pillars of our trustworthy AI engineering framework.

2.1. Models and Explanations

Explicit models\textsuperscript{2} of the world or a suitable context in question enable reliable predictions of the behaviour of AI systems, both in the scope of training and outside, because they generalise knowledge beyond the limited and biased scope of the training data. Given a certain context, which can be very narrow or broad, explicit models represent concepts, relationships and rules that are always true in that context. For example, the laws of gravity are applicable to the whole universe. Models can be created by experts or learned from experience and data. Combinations of different types of models are particularly useful and insightful. For example, neuro-symbolic approaches are used to achieve this [13, 14, 15, 16, 17]. In this way, models promote transparency and explainability and, thus, make it possible to render the behaviour of the AI systems understandable and plausible. In simulations, models can enable the understanding – through experiments – of situations that are difficult or impossible to access otherwise. Often, synthetic data can be used to maintain privacy and avoid dangerous conditions.

Because models depend on a given context or domain, it is essential that agents using those models are aware of their competence in the given situation and are able to apply suitable models or adapt to situations gracefully when changing or leaving their scope of competence.

2.2. Causality and Grounding

Causality refers to the ability to identify and predict cause-and-effect relationships, i.e. which effects are the results of which causes and why [18]. An AI system that can understand causal relationships is able to make informed predictions and solve complex problems.

The need to move from correlation to causation is increasingly urgent (see figure 1, where the dotted line indicates correlation and the arrows indicate asymmetric causal relationships). If we want to explain why certain predictions are made or decisions are taken, it is essential to know and act on their causes.

\textsuperscript{2}The term ‘model’ is used extensively in the ML community. It is necessary, however, to distinguish between the statistical models of ML and the semantic models of knowledge engineering. Here, we refer to the latter. See also in [12] for a unified taxonomy of AI.
Causal inference is concerned with the resulting effect when a corresponding event (cause) occurs, according to a given causal model. Causal inference asks whether an event indeed causes a certain effect by determining the likelihood that one event was the cause of another. In contrast to statistical correlations, causal relationships are directed and asymmetrical.

Counterfactuals refer to alternative choices that could have been made in the past and the corresponding effects that they might have caused. Therefore, they allow for exploring possibilities to find alternative outcomes according to a causal model, allowing to change policies accordingly in the future.

Causal discovery allows for determining whether a change in one variable (representing a state, action or event) indeed causes a change in another, in order to distinguish between correlated and causal relationships in data and to derive corresponding causal models.

Closely related to causality is understanding the anchoring (grounding) of meanings in the real context. A deep understanding of context and meaning requires not only processing data, but also capturing the real-world phenomena that the data represents, such that predictions, decisions and actions are based on them. Layers of abstractions are fundamental for building rich architectures. Semantic models, such as ontologies, are representations of concepts, their attributes and relationships. They contribute to trustworthy AI systems by explaining and constraining the meaning of those concepts.

2.3. Modularity and Compositionality

One of the fundamental design principles of (software) engineering is modularity. Modularity guarantees that complex systems are broken down into understandable and manageable parts (functions and features) and assembled into system architectures. This increases the reliability of the individual components and their assemblies as systems of systems. It is much easier to verify smaller components than big monolithic artefacts. The evolution in software engineering from structured to modular and object-oriented programming enabled the design and construction of complex systems. In well-designed systems the transitions between successive components can be controlled and protected, making them explainable such that errors can be detected and repaired effectively. The pre- and post-conditions of each component can be validated and orchestrated in increasingly complex systems of systems.

When designing trustworthy AI systems, there are several important aspects that should be considered to guarantee the characteristics of trustworthy AI. In principle, these aspects apply to all software systems. However, they are of the greatest relevance for complex, intelligent systems for critical applications. AI engineering should make use of the lessons learned from software engineering and apply its engineering principles, such as design patterns and architectures.

An attempt to model design patterns for neuro-symbolic systems is made in [12, 19]. Two examples (see figure 2) show data-driven and knowledge-driven patterns. They are based on a visual language and taxonomy.

An important advantage of modular systems is that compositional patterns of subsystems can be identified and defined, which increases their reliability and documentation through reuse [20].
Figure 2. Modular Design Patterns for Hybrid Learning and Reasoning Systems

It is important to stress that software architectures are not merely static artefacts, but they rely on the interplay between structures and events – the organising principles and the dynamic evolution of complex systems [21]. Neither structure nor events are meaningful on their own, but require and depend on each other. In an extrapolated view, this relationship may be applied to the combination of learning and reasoning. Meaning emerges from a system’s structure and its components, when it is operated in a dynamic context of perceiving and acting.

The principle of compositionality also applies to knowledge models and languages [22]: larger constructs are created by joining together smaller units with specific, understandable, and verifiable tasks. Abstract relationships can thus be traced back to their components. These aspects are applied when designing complex systems and should also become a matter of course for AI systems.

2.4. Human Agency and Oversight

Human agency and oversight mean that, in any case, a human being should have the overview, final decision, and responsibility for the actions of an AI system (human empowerment). Even if many tasks are increasingly being transferred to autonomous AI systems (agents), the principle that humans supervise, assess, and approve actions still applies. Keeping in mind the above-mentioned dilemma in building trustworthy AI systems, delegation of tasks needs to be interpretable by both humans and (software) agents – in particular, when humans and agents collaborate as hybrid teams in a symbiotic partnership. It is necessary that suitable task descriptions are handed over to the agents and that they understand and execute them in the relevant context, considering the models, explanations and causal relationships explained above.

When considering the collaboration and competition in hybrid teams of humans and autonomous agents, we consider many-to-many situations where multiple humans and multiple agents form hybrid teams. The purpose of the agents is to empower humans with providing their complementary capabilities, such as fast and precise information exchange and analysis of large data sets. Agents can play many different roles, but the responsibility for decisions remains, in principle, with humans, for example by verifying, validating and approving proposals for decisions. An essential aspect of meaningful collaboration is to make mutual assumptions and expectations explicit, such that they can be used in deliberation and communication. This is a prerequisite for appropriate delegation of tasks and the accurate and concise descriptions of their underlying intentions.

For collaborative decision-making (CDM), it is essential that each human and agent is aware of each others’ points of view and has a notion of the others possess points of view that might differ from one’s own - which is known as a Theory of Mind (ToM). ToM is defined as the human cognitive ability to perceive and interpret others in terms
of their mental states and it is considered an indispensable requirement of human social life [23, 24, 25, 26, 27, 28]. Rather than reasoning only with one’s own beliefs, desires, goals, intentions, emotions, and thoughts, a person or agent with the awareness of others’ states of mind can consider different and mindful acts, depending on a perceived context. This ability allows them to more easily understand, predict, and even manipulate the behaviour of others [29].

Trustworthiness in interacting with artificially intelligent systems emerges from experience and as a combination of various properties, such as fairness, robustness, transparency, verification, and accuracy [30]. AI systems are trusted when we have confidence in the decisions that they take, i.e. when we understand why they are made [31], even when we disagree.

2.5. Maturity Models

Maturity of software is commonly denoted by means of Maturity Models[^3], which are frameworks that can be used in the process of planning and engineering, as well as in the process of road mapping. An extensive overview of AI maturity models is written by Sadiq et al [32].

In previous work [33] we presented a maturity-model that expressed the level of cooperation of an AI entity (agent) that acts in a human-AI team. The model can be used to reflect on expected capacities, roles and responsibilities of AI entities that act in a Human-AI team. The maturity model classifies the level of cooperation along two dimensions, level of agency and level of communication. It was represented by means of a two-dimensional matrix.

Horizontally, levels of agency range from human-controlled to fully autonomous [34, 35, 36]. Artificial Intelligence is based on the principles of autonomy and agency. Autonomy, the quality or state of being self-governing, is required to avoid purely predictable and reactive behaviour [37]. Whenever an AI entity commits on contributing to a team intention, it has to balance its level of autonomy with required levels of interaction. The model distinguishes four levels of agency with respect to an AI entity acting in a team (Human Trusted, Situational Autonomy, Preferred Autonomy and AI Trusted).

Vertically, levels of communication vary from merely sharing information about alignment of tasks, to forms of interaction in which an agent takes into account the mental state of others. Communication is a prerequisite for deliberation, delegation of tasks and sharing of knowledge within an ecosystem. We distinguish four levels of communication, varying from simple sharing information about coordination of tasks to higher orders of interaction that include the exchange of information about the learning process and each others’ mental states. The maturity model distinguishes four levels of communication (Task Alignment, Co-Learning, Mental Modelling and Motivating).

We extended the maturity model with a third axis (see figure 3). The maturity model, named the AI Interaction Maturity Model, manifests itself in the form of a three-dimensional cube. The third axis can be used to express the impact of a particular AI team member on the social level, varying from an individual level (silos situation) to organisational, industrial domain-specific and societal level.

[^3]: Another note on the term ‘model’, as it is an ambiguous term; whereas in software engineering it may refer to a computational model, theoretical model or architectural model, we use the term model here to refer to an engineering framework, commonly denoted with the term ‘maturity model’.
Figure 3. The AI Interaction Maturity Model extends the Collaborative Agent Maturity Model by including a third axis that reflects the impact of an AI entity on the social level.

Figure 4. A causal model for living and working in the urban context.

3. Trusted Urban AI Scenario

As an example for applying the above-mentioned AI engineering concepts, we propose a scenario in an urban context.

Urban life has many peculiar characteristics [38, 39, 40, 41, 42, 43]. Some causal relationships in an urban context, focusing on energy consumption and mobility, are shown in figure 4. We are concerned with modelling and understanding human behaviour in an urban context (sustainable smart city), particularly when humans are part of hybrid teams together with agents.
The interactions in an urban environment are diverse, complex and conflicting. Many interests of hybrid actors are related and depend on each other. In the urban context, an overall goal for sustainable use of resources could be the reduction of energy consumption.

Using causal models, adopting and implementing the engineering disciplines and using a maturity model, as explained above, improves our understanding and control of systems that we design and apply in this urban context. The consumption of various types of energy is affected by the need and desire to move about the city and to heat buildings at home and at work (and for leisure, shopping, etc.). As shown in fig. 4, values and duties are the main sources that drive urban behaviour and external factors, such as the weather, influence decision-making. This causal model explains the relationships among several important behavioural aspects, but it is not deterministic. Individual behaviour is influenced by exogenous variables and cooperative behaviour results in complex interactions. A shared goal can be seen and modelled as an effect, that is caused by one or more interventions (actions or events). Consequently, in order to decide and plan which actions to take, it is necessary to understand which actions or events cause the intended effects. For example, your goal can be to arrive at a destination at a given time (work, home, leisure, etc.). By reasoning back which actions are required to get you there, piece by piece, a connected causal path can be constructed to determine the departure time and modes of traffic along the route. Due to shared intentions and causal models, humans and agents can mutually trust each other regarding their actions and outcomes.

The urban context comes with a multidisciplinary stakeholder field, involving a landscape of IT systems varying from traditional components in data sharing platforms to AI-enabled services. A modular approach for both design and realisation of software modules and AI models is crucial to keep the systems at their required levels of interoparability and scalability. Roadmapping of AI based systems, inside buildings as well as between various buildings and their interaction with human engineers is facilitated by means of the AIMM model.

4. Conclusions

As the field of Artificial Intelligence is still, and again, facing tremendous and overwhelming changes and progress, there is a strong and quickly growing need for trust in AI systems. The goal of Trust by Design is proposed to be based on the five engineering principles of (i) Models & Explanations, (ii) Causality & Grounding, (iii) Modularity & Compositionality, (iv) Human Agency & Oversight, and (v) a Maturity Model. Our intention is to develop the insights above further into practical methods and tools, based on a design pattern language, to benefit the AI community and its users. The context of energy consumption and mobility in an urban context serves as applied setting setting in various projects, validation of our suggested 5 pillars for controlled engineering and further experimentation in the field of human-AI ecosystems.

Acknowledgements

This research was partially supported by TAILOR, a project funded by EU Horizon 2020 research and innovation programme under GA No 952215.
References


33. Mulder W and Meyer-Vitali A. A Maturity Model for Collaborative Agents in Human-AI Ecosystems. *Collaborative Networks in Digitalization and Society 5.0*. Ed. by Camarinha-Matos LM, Boucher X, and Ortiz A. IFIP Advances in Information and Communication Technology. Cham: Springer Nature Switzerland, 2023: 328–35. DOI: 10.1007/978-3-031-42622-3_23


