



Generative AI: Considerations for Use in Corporate Enterprises

September 7, 2023



Agenda

- Welcome & Introductions
- History and Definitions
- Security Considerations
- Possible Applications
- Q & A
- Wrap-up

Code of Conduct

GDG Twin Cities is dedicated to providing a harassment-free and inclusive event experience for everyone regardless of gender identity and expression, sexual orientation, disabilities, neurodiversity, physical appearance, body size, ethnicity, nationality, race, age, religion, or other protected category. We do not tolerate harassment of event participants in any form. We take violations of our policy seriously and will respond appropriately.

Emily Anderson
Application Developer, Consultant Blue
Shield of California

Previously:

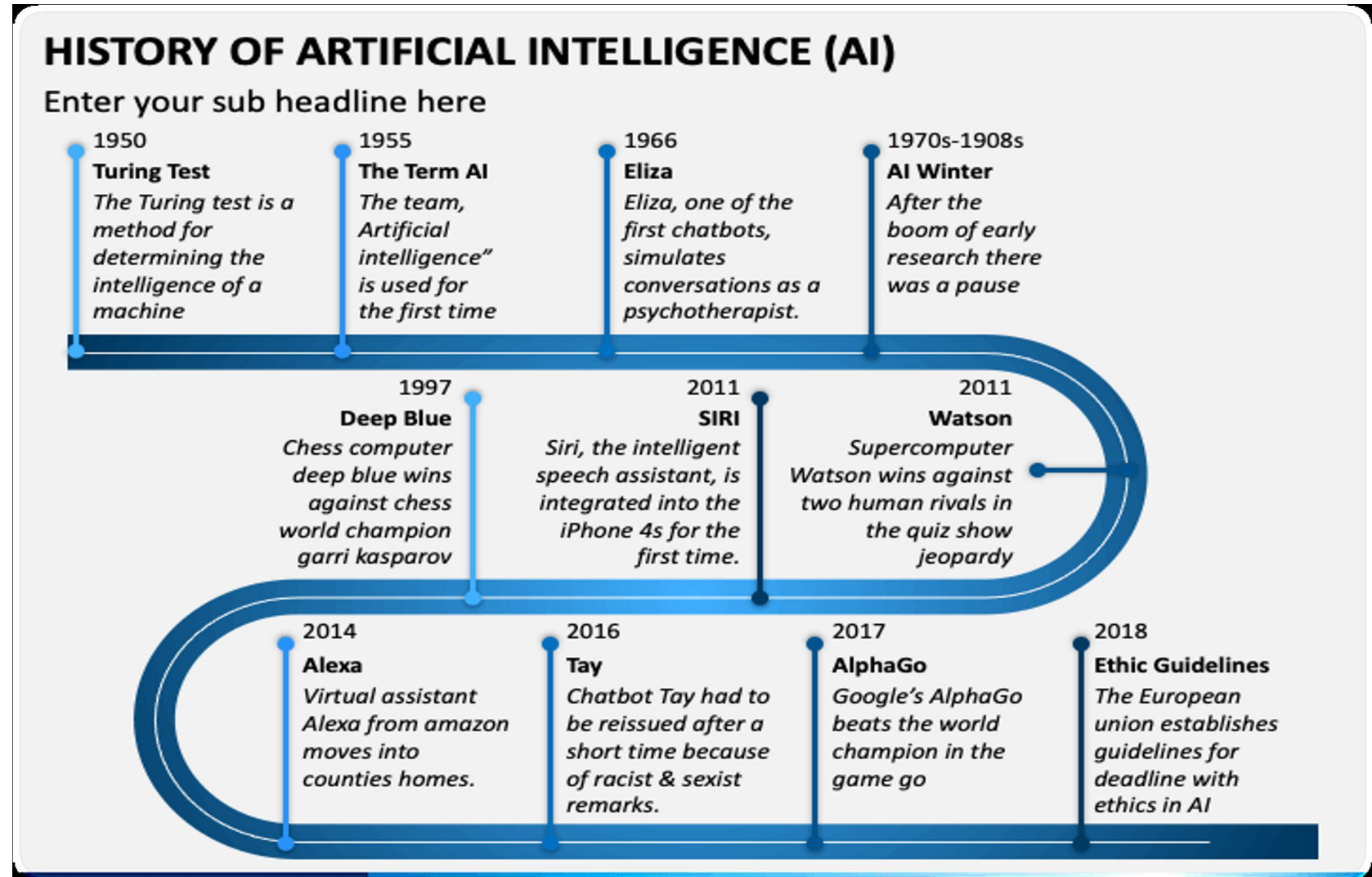
- Rules Analyst/Product Owner - Florida Blue
- Business Rules Developer - Aetna: A CVS Company
- Rules Developer, Database Developer, Help Desk Lead
-State of Minnesota
- Social Worker - Crow Wing County





History and Definitions

History & Background



The terminology around Generative AI

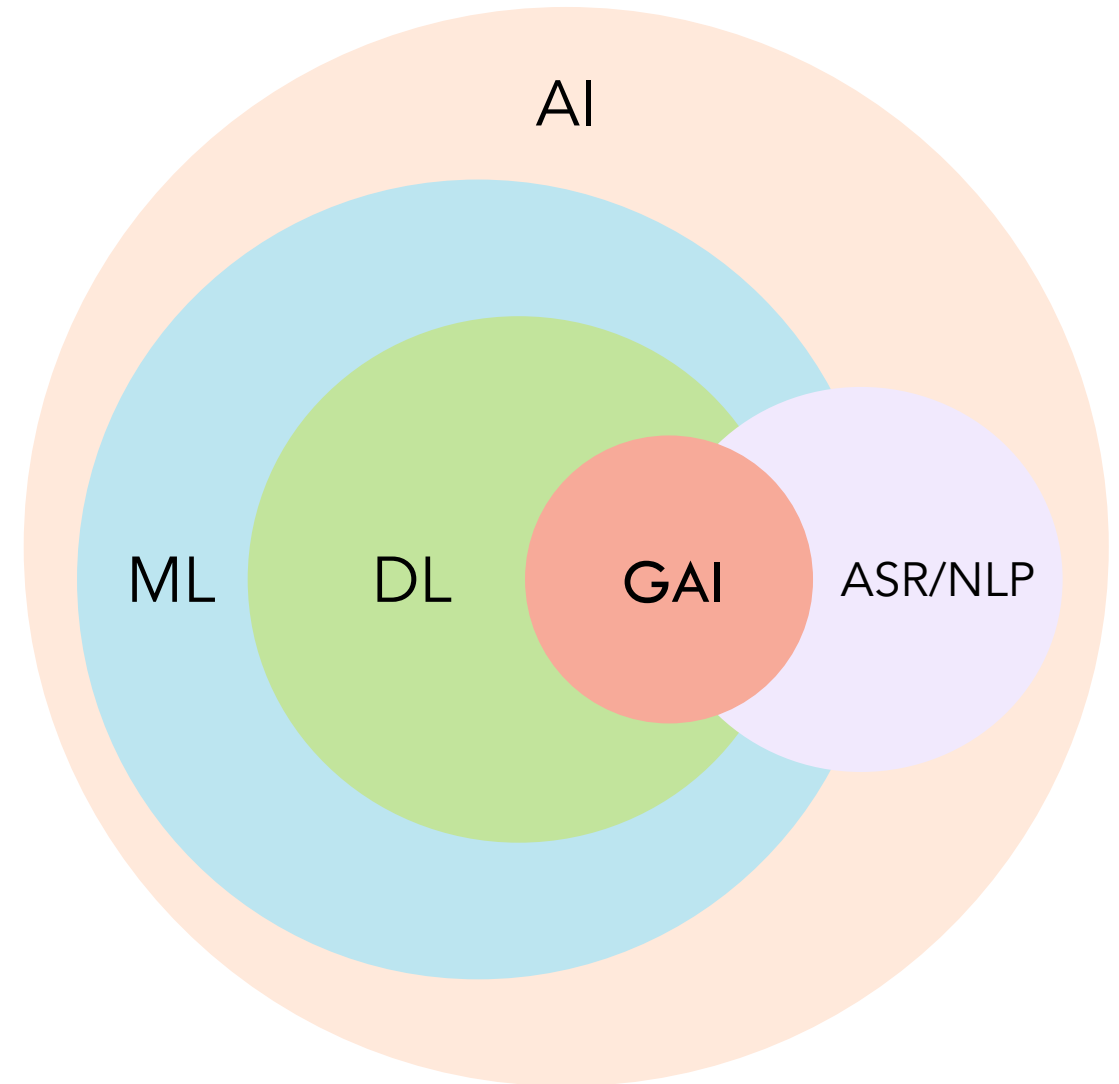
AI: **Artificial Intelligence** is the simulation of Human Intelligence

ML: **Machine Learning** is a type of AI, which uses data and algorithms to imitate human learning, gradually improving its accuracy.

DL: **Deep Learning** is a type of AI & ML that teaches computers to process data. DL models recognize complex patterns to produce increasingly accurate insights and predictions.

GAI: **Generative AI** is a type of AI that uses ML algorithms to create new and original content based on input data.

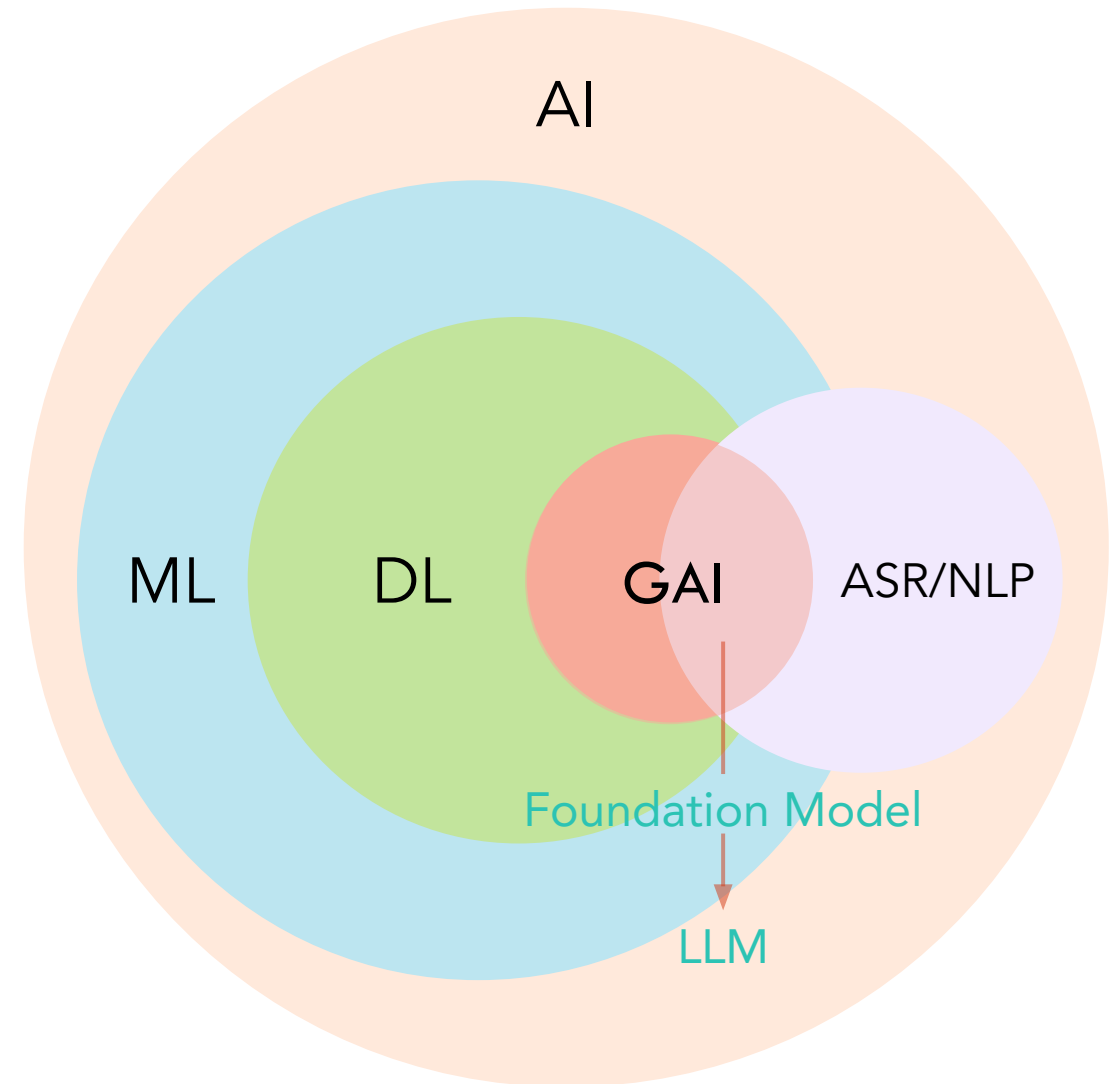
ASR/NLP: **Automatic Speech Recognition, Natural Language Processing**, is a branch of AI, giving computers the ability to understand text and spoken words the way human beings can.



Two terms that are crucial to understanding GAI

FM: **Foundation Model** is a ML model, pre-trained on massive unlabeled datasets, that can be adapted for **problem solving**. (E.g.: BERT, GPT3)

LLM: **Large Language Model** is a type of FM that works specifically with **language**. (E.g.: ChatGPT, Google's PaLM, Meta's LLaMA)

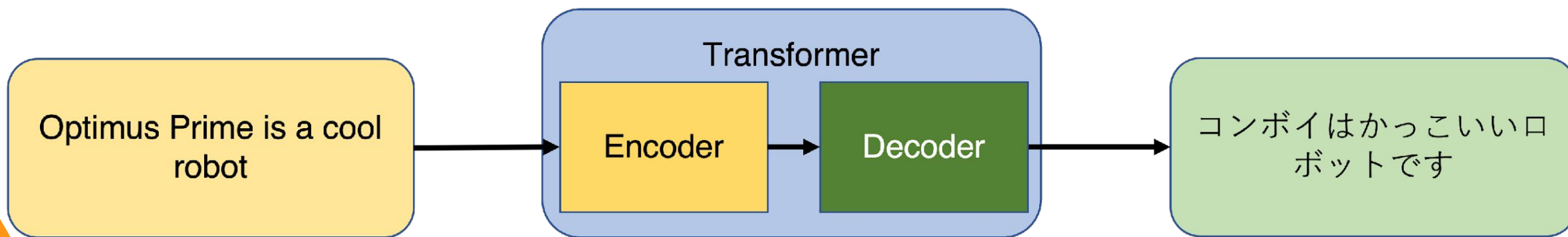


The Introduction of Transformer Technology enabled LLMs to go mainstream

Introduced by Google in 2017.

Transformers differ from prior architectures in their ability to [assign context](#), [track relationships](#), and [predict outcomes](#).

Transformers enabled AI to move beyond the limited pattern-spotting into the creation of expressions of content.





Foundation Models

How are companies incorporating Foundation models in every-day business?



Microsoft: Microsoft 365 Copilot — your copilot for work. It combines the power of large language models (LLMs) with your data in the Microsoft Graph and the Microsoft 365 apps to turn your words into the most powerful productivity tool on the planet.



Salesforce: Salesforce announced its partnership with ChatGPT and introduced its own Einstein GPT, a tool based on OpenAI's chatbot to create the first generative AI for its customer relation management (CRM) tools



Air India: Uses ChatGPT to improve the customer experience on its website. The airline will reportedly use the latest version of ChatGPT, GPT4, to improve the FAQ section, pilot briefings, and more.



Snapchat: The company has introduced a ChatGPT-powered AI chatbot named "My AI." My AI is currently available only to Snapchat Plus subscribers and is a toned-down version of ChatGPT.



Duolingo: Language learning app Duolingo has announced Duolingo Max, a subscription service that offers tailored lessons to users to help them learn easily. Duolingo Max uses GPT-4 to allow users to ask questions such as "Explain my answer" and "Roleplay."



Slack: In addition to using ChatGPT for its CRM, Salesforce also integrates ChatGPT with Slack. Slack users will get access to a new assistant dubbed as "Einstein" that will help users draft replies, summarize threads, research on a particular topic and more



Bain & Company: Global management consulting giant Bain & Company has partnered with OpenAI to integrate its AI chatbot into its management systems.




Security Considerations

Risks to Consider

Data Risk	Model and bias risk	Prompt of input risk	User Risk
<ul style="list-style-type: none">• Errors in propagation of AI Models• Misleading or harmful content• Unauthorized secondary uses of data• Contractual issues• Privacy-disclosure of unauthorized data sets through AI models	<ul style="list-style-type: none">• Breach of ethical and responsible AI principles in the language model development, leading to discriminatory or unfair outputs• Human-cognitive biases relate to how an individual or group perceives AI system information to make decisions	<ul style="list-style-type: none">• Misleading, inaccurate or harmful responses due to unsophisticated prompts or questions being provided to the AI model	<ul style="list-style-type: none">• Unintended consequences due to users becoming unknowing parties to the creation of misinformation• Harmful content

Security Safeguards


Automate, update, and upgrade cyber countermeasures.	<ul style="list-style-type: none">• Continuously assess access privileges on a user-by-user basis to identify probable attack vectors and chains powered by generative AI.• Ramp up detection countermeasures. Build an endpoint detection and response (EDR) platform using generative AI to detect anomalies with few to no false positives.• Continuously evaluate the models' vulnerabilities to adversarial attacks in different domains using emerging evaluation toolkits.
Prepare for higher-resolution threat models and insights, predictions and scenarios.	<ul style="list-style-type: none">• Analyze collected vulnerability data and compromise assessment data, and draft assessment reports and remediation plan/activities.• Generate executable threat scenarios specific to your company's environment and identify most effective mitigation strategies.
Put data loss prevention controls in place.	<ul style="list-style-type: none">• Establish controls to manage public use of your generative AI.• Identify potential exfiltration of generative AI-related data.• Use generative AI-focused data protection processes to see and safeguard sensitive data in use, in transit and at rest.• Identify privacy and other data-risk controls needed to use generative AI in a risk-based manner.
Protect internal/local generative AI models and associated data.	<ul style="list-style-type: none">• Put controls in place to protect the models against misuse and unauthorized use, in line with the company's legal, privacy, security and ethics policies and procedures.• Create internal security controls around generative AI tools to prevent manipulation of data in models or unauthorized use that may cause these tools to deviate from intended parameters.• Understand the security posture and controls used by vendors of your internal generative AI instances and related data environments that you use and correct where needed.



Possible Applications



Applications to Healthcare

- Diagnosis and treatment: AI can be used to help doctors diagnose diseases more accurately and quickly. AI can also be used to develop personalized treatment plans for patients.
 - Personalized medicine: AI can be used to create personalized treatment plans for patients based on their individual genetic makeup, medical history, and other factors. For example, AI-powered systems can be used to recommend the best course of treatment for a patient with cancer.
 - Healthcare administration: AI can be used to automate many of the administrative tasks associated with healthcare, such as scheduling appointments, processing insurance claims, and managing patient records. This can free up healthcare workers to focus on providing care to patients.
 - Patient education: AI can be used to create personalized educational materials for patients about their condition and treatment options. For example, AI-powered systems can be used to create interactive educational games and videos.
 - Reduced costs: AI can help to reduce the costs of healthcare by automating tasks, improving efficiency, and reducing errors.
 - Improved patient experience: AI can help to improve the patient experience by providing more personalized care, making it easier to access healthcare, and reducing wait times.
- 

Brainstorm possible applications in your
area of business
(Ask Bard for suggestions!)

Consider risks and security concerns

Share!





Q & A



Thank you

@e_s_anderson

LinkedIn: emilyanderson81

anderson.emily.sue@gmail.com