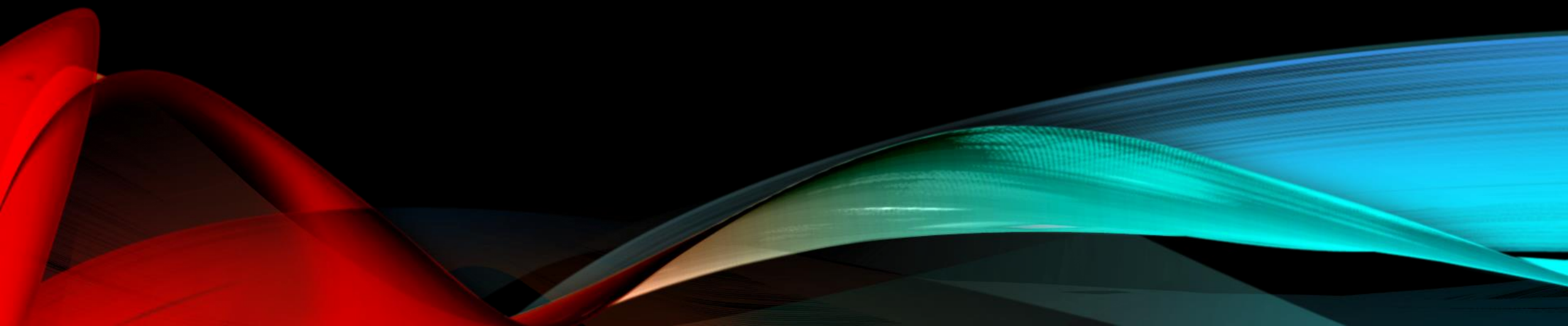
REQUIREMENTS ENGINEERING FOR AI

Ada Yetiş

WHAT IS REQUIREMENTS ENGINEERING?



- The process of defining, documenting, and maintaining what a product or service needs to be.

Elicitation

- Collect requirements from many relevant sources
- This does not produce formal models, simply increases domain knowledge

Specification

- Produce formal software requirement models
- Includes all functional and non-functional requirements and constraints

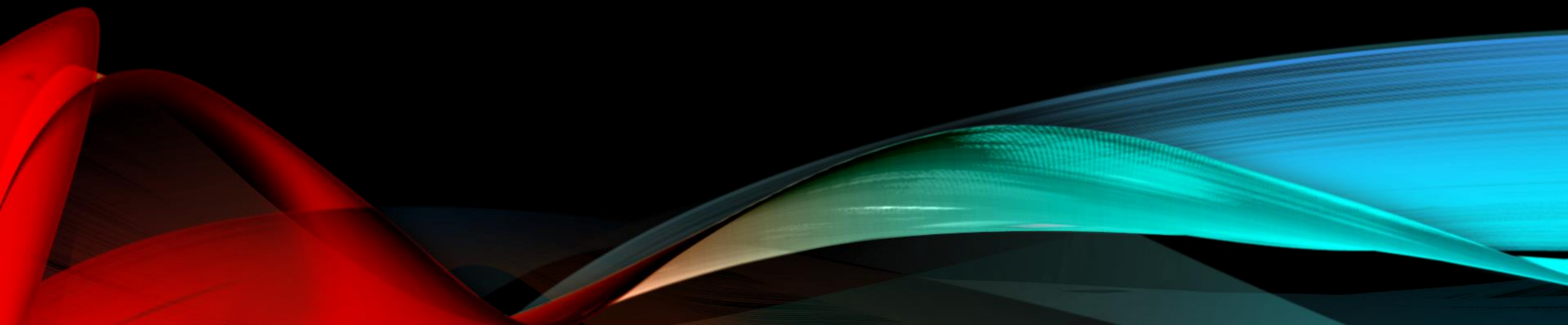
Verification and Validation

- Ensures that the software correctly implements a specific function
- Ensures that the software that's been built is traceable to customer requirements

Management

- Process of analyzing, documenting, tracking, prioritizing, and agreeing on requirements
- Ensures that the requirements are modifiable in later stages

IS THIS ENOUGH FOR AI?



WHAT'S DIFFERENT?

- Machine learning generates rules based on examples and a fitness function
  - Behaviour is no longer a result of manually coded rules.
  - The predictive power of machine learning systems comes mostly from the training data, not the source code.
  - The model is more opaque, the behaviour can no longer be traced to human readable functions.
- Most decisions in machine learning systems are made by data scientists
  - They define fitness functions, select and prepare data, assure quality etc.
  - These decisions should be based on an understanding of the business domain and stakeholder needs.

WHAT'S MISSING?

Quantitative Targets	•Makes expectations explicit •Picking the correct evaluation metric is extremely important
Explainability	•The systems are much more opaque •Makes the decision making process hard to understand
Freedom from Discrimination	•The nature of ML systems bring out stereotypes and biases in data •It's important to account for this while choosing the data
Legal and Regulatory Requirements	•The models are trained on personal data, which requires explicit consent
Data Requirements	•The data determines what the system does as much as, if not more than, the actual model. •So data needs to be held to the same requirements as the system itself.

QUANTITATIVE TARGETS

- Quantifies qualitative targets
  - Allows for the communication of expectations between the development team and the client
  - Important for normal software as well but crucial for machine learning systems (and much more complicated)
- The evaluation metric of the model needs to be specified.
  - There are multiple measures that can be used to quantify the predictive power of a system.
  - Not all measures are equally good for all systems.

EXPLAINABILITY

- Machine learning systems are, by nature, opaque
  - The decision algorithm is generic and the results depend on data
  - This contrasts with conventional software where the algorithm is a direct reflection of the decision making process
- Determining what to explain is important
  - The user might need to understand certain aspects of the model or predictions without necessarily having to learn all of it.
- Making the model explainable also requires keeping the model simple.

FREEDOM FROM DISCRIMINATION

- Machine learning algorithms extract biases and patterns from the data.
  - This makes them susceptible to learning and exacerbating pre-existing biases and stereotypes in data
- This is an important requirement to ensure that the system only uses socially and legally accepted qualities to make it's predictions
- It's a bigger issue in machine learning systems because:
  - It's a lot more implicit
  - The algorithm amplifies the discrimination bias in the data
- The characteristics that shouldn't be used must be determined
  - They can be removed from the training data
  - A feature analysis can be performed on the model to determine which features are being used by the system

LEGAL AND REGULATORY REQUIREMENTS

- Models are trained on personal data
  - Users must explicitly consent to having their data used and the ways in which the data will be used
- It's important to track legal requirements and ensure that no illegal features have been used to train the machine learning models.

DATA REQUIREMENTS

Data quantity

Requirements should be specified on the diversity of the examples and not the number

Additional data sources must be identified and used

Data quality

Completeness

Does the data cover the full range of values?

Consistency

Is the format and representation of the data the same?

Correctness

Is the data true?

Elicitation

- Collect requirements from many relevant sources
- This does not produce formal models, simply increases domain knowledge

Specification

- Produce formal software requirement models
- Includes all functional and non-functional requirements and constraints

Verification and Validation

- Ensures that the software correctly implements a specific function
- Ensures that the software that's been built is traceable to customer requirements

Management

- Process of analyzing, documenting, tracking, prioritizing, and agreeing on requirements
- Ensures that the requirements are modifiable in later stages

REQUIREMENTS ENGINEERING FOR AI

Elicitation

- Elicit additional data sources
- Data scientists and legal experts should be consulted at this stage
- Protected characteristics and explainability requirements should be identified

Analysis

- Define and discuss performance measures and expectations
- Define and discuss conditions for data preparation, definition of outliers, and derived data

Specification

- Must include specifications for all the things discussed above

Verification and Validation

- Validation must be performed throughout the life of the system.
- A retraining schedule must be created by analyzing the problem domain
- Data anomalies and the resultant unexpected behaviour must be specified
- Training and production data must be analyzed for biases