GOING FROM RISK TO QUALITY OF AI

Sander Mol

Workgroup Testing and AI

Warning: This presentation is about AI and therefore contains cat pictures and Skynet.

This presentation on YouTube (Dutch):

https://www.youtube.com/watch?v=yuhDuCxZMuA

Our previous presentation on YouTube (Dutch):

https://www.youtube.com/watch?v=iHG64_Czmps

All of our other work (also in English):

https://www.testnet.org/testnet/p000610/werkgroepen/werkgroep-testen-en-ai

Our workgroup

Rik Marselis

Martin van Helden

Marco Verhoeven

Richard van Emmerik

Mariëlle van der Sluys

Johannes Sim

Peter Collewijn

Gerline van Lieburg

Hannie van Kooten

Sander Mol

Members

Agenda

The basics: Machine Learning and Deep Learning

Five risks of AI

How to test AI

The basics: Machine Learning

Our starting point: a fixed algorithm

The predicted house price in euros =

700 * living area +
500 * plot area +
8,000 * number of bedrooms +
score based on zip code

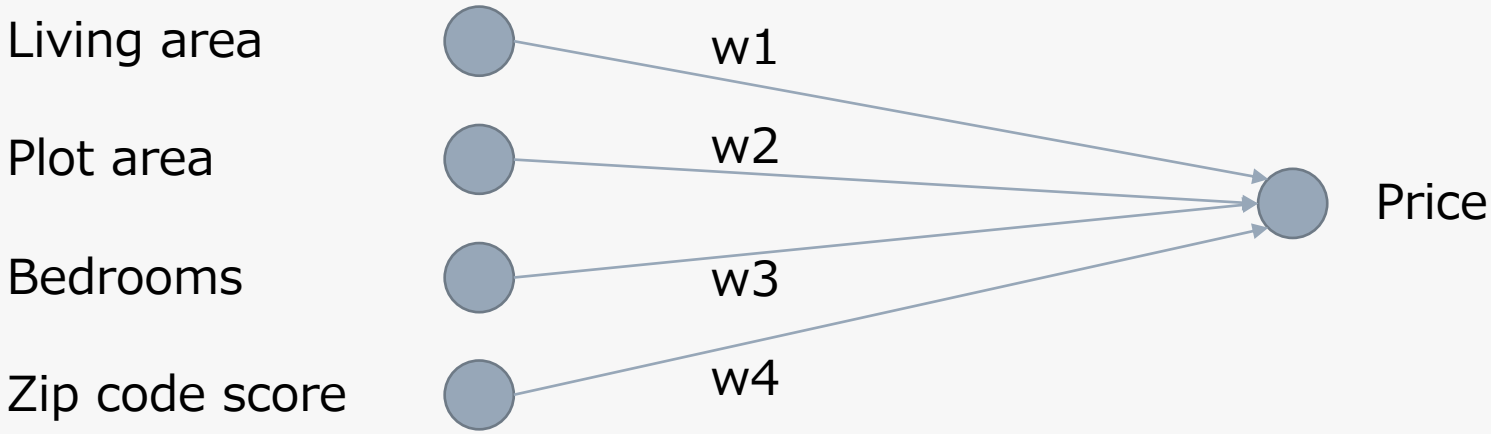
The basics: Machine Learning

A new starting point: data

Living area	Plot area	Bed-rooms	Zip Code (NL)	Price
110	173	4	3311 AA	400.000
104	145	6	3351 ES	375.000
122	211	5	3352 VA	450.000
...	...	...	...	...

The basics: Machine Learning

A learning algorithm



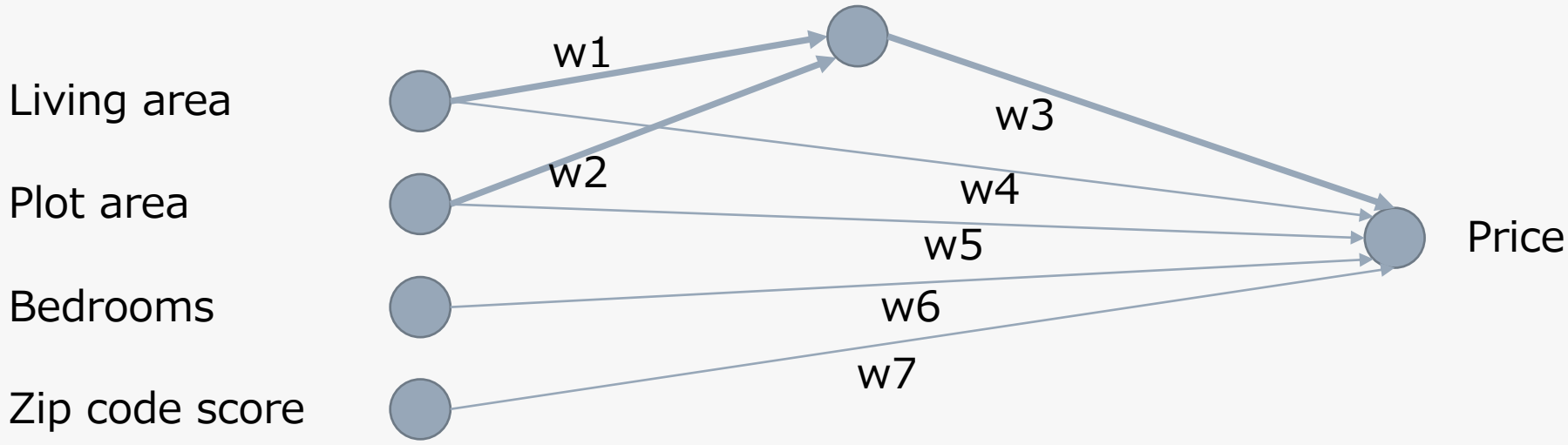
The basics: Machine Learning

Learning the right weights

- Enter any weights
- Repeat the following
  - Calculate the price based on these weights
  - Compare the calculation with the correct price
  - Adjust the weights a little bit
  - See if the predicted price gets a little better
  - Store the best weights

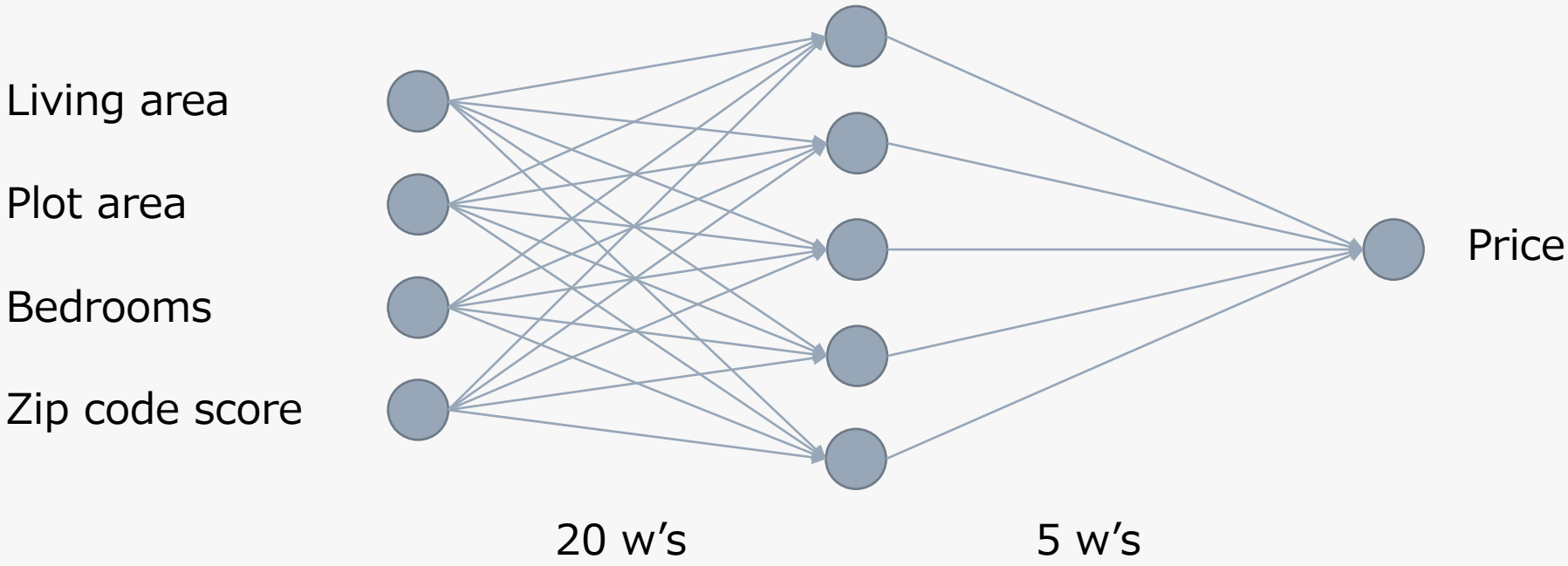
The basics: Deep Learning

A learning algorithm



The basics: Deep Learning

A learning algorithm

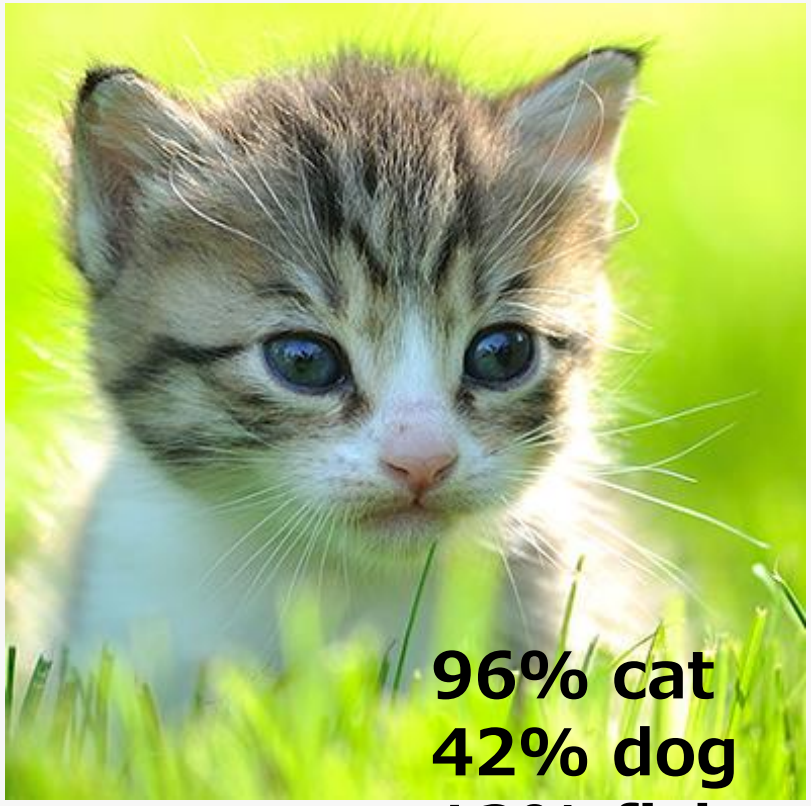


Five risks of AI (ML)

Risk 1: uncertain outcomes

For house prices (i.e. 'regression'): the variables enter a model and a fairy logical price comes out. But no exact expected value.

With cat pictures: the picture goes into the model and a percentage of certainty comes out. This is never 100%! What percentage is good enough?



Five risks of AI

Risk 2: dependence on data

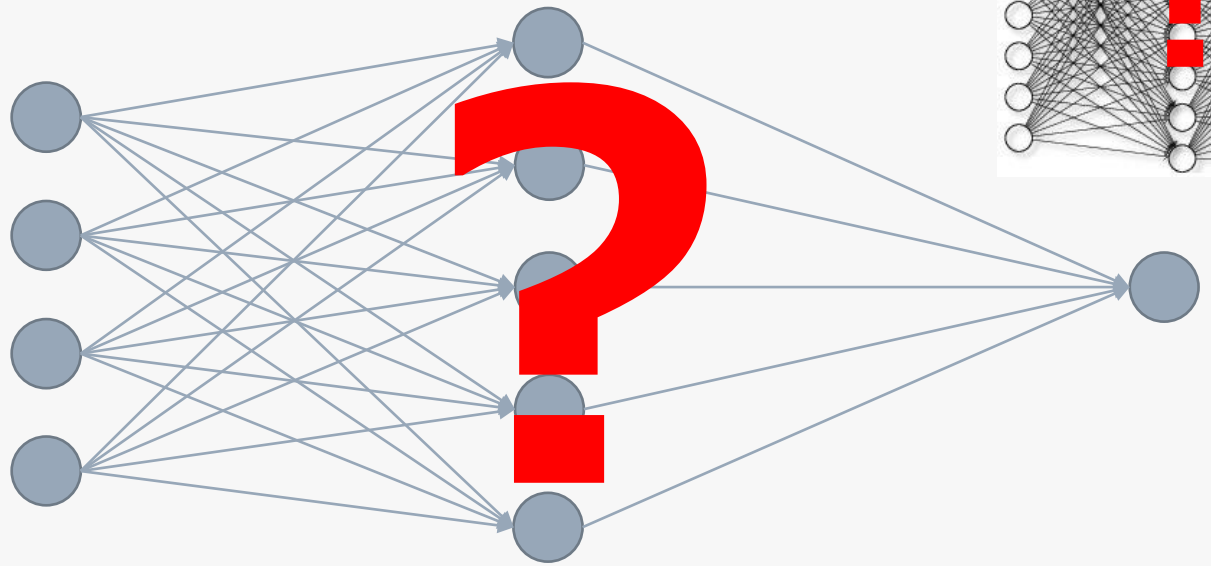
Data is often:

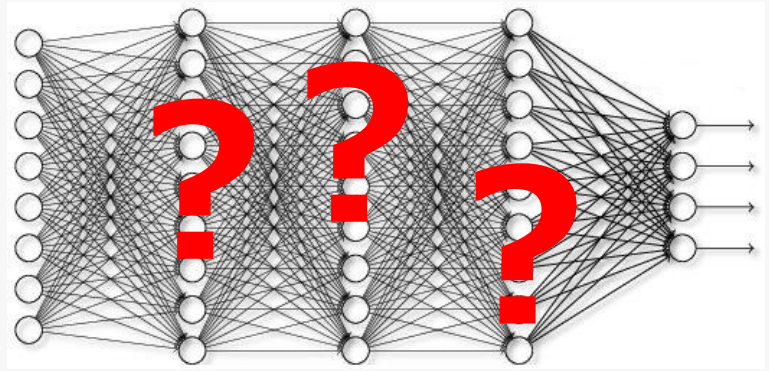
- deprecated
- incomplete or incorrect
- selectively collected
- open to interpretation
- and it sometimes shows patterns that we don't like very much

64% cat ?

Five risks of AI

Risk 3: limited explainability





Five risks of AI

Risk 4: changing reality or needs

Changing reality: house prices! But also legislation, trends, development of new words, changes in assortment, and so on.

Changing need: “How handy that we can recognize car window damage, just do the same for buses, homes and greenhouses.”

Five risks of AI

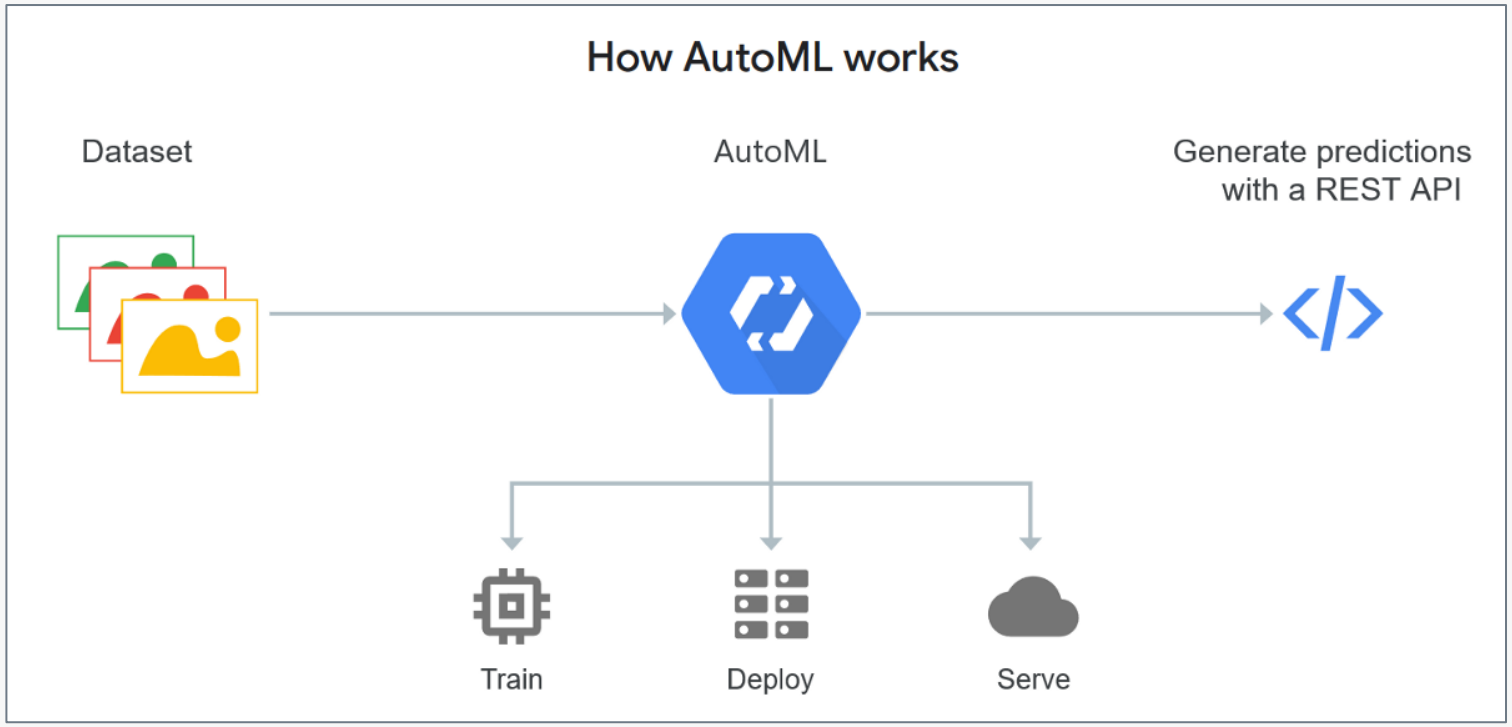
Risk 5: General fear of AI

Sometimes because of previous **bad experiences** with AI implementations that were too fast, or because of knowledge of what **uninhibited application** can do.

Sometimes based on **ignorance**, possibly combined with **doomsday scenarios**: suppose that the AI can not only learn, but can also reason, understand context and develop standards and set goals itself.

Five risks of AI

Bonus risk: quick to make, difficult to test



How to test AI (ML)

Test your data!

Ask all the important questions about data:

- Is it current and representative?
- Does everyone interpret the data the same?
- Are the operations logical and consistent?
- And so on.

How to test AI

How to test representation :

Check that all field values (input and output) are properly represented. Also check the differences between test and training set.

If necessary, go a step deeper, for example with pairwise testing.

You can also talk to 'the business' about what a good data distribution is. You can do this with the Data Combination Test!

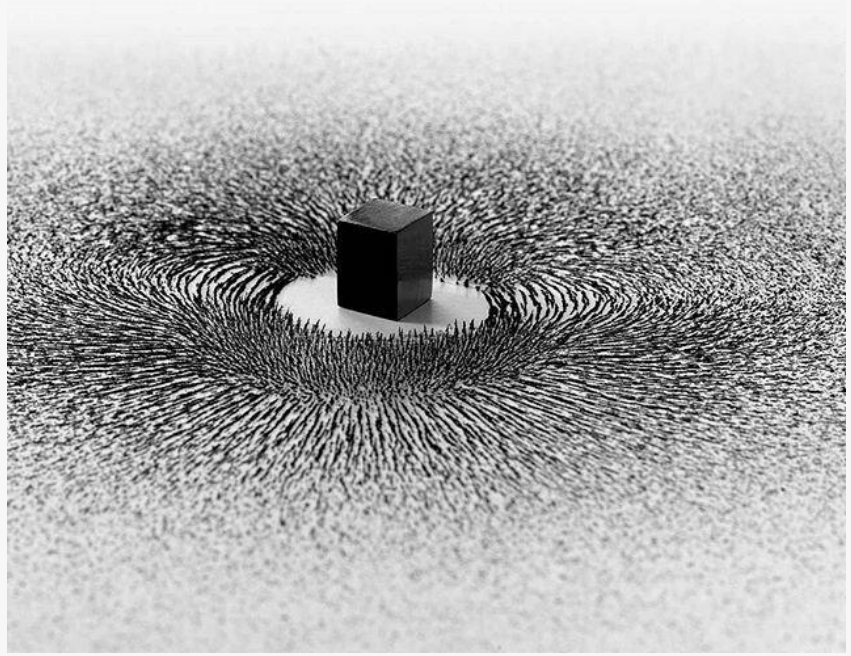
(a representative business pair)

How to test AI

Don't test outcomes, test patterns

Adjust the input data a little and see if the output changes well. So for house prices: with a **larger plot area** you would expect a **higher price**.

Metamorphic testing: testing relationships.



How to test AI

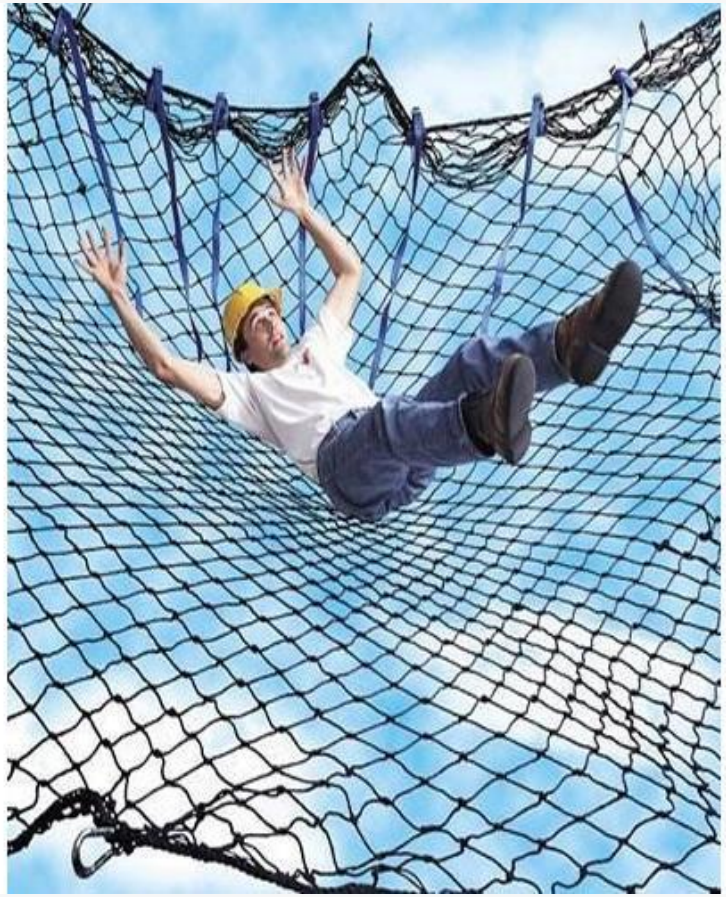
Testing for robustness

Handling extreme values. Or 'safety nets'.

Recognition if someone tries to play the AI.

Test AI in the chain: are all input and output variants handled properly?

- input: all minimum data entered? Logical combination of data?
- output: confirmation email with license application, notification if no suitable product to recommend, and so on.



How to test AI

Test for interests

The AI can provide all possible outcomes, make sure that different target groups are well served based on examples.

Create personas and link them to use cases!

How to test AI

Let people watch the process!

Digging in data is great fun, but ultimately actual people will have to work with it. Show users and their managers the development process.

Make sure all expertise is involved. Take the ideas of experts and address their concerns.

How to test AI

Read the guidelines

The conditions for making AI useful and fair have been considered for a long time.

- Within the government (EU, Netherlands)
- Within branches and professional associations
- Within organizations

Yes, uniformity is certainly needed, but there will surely be useful tips to be gained from it! In addition, government guidelines will one day become the basis for laws and regulations.

Everything on one slide

Risico’s

- Uncertain outcomes.
- Dependence on data.
- Limited explainability.
- Changing reality or need.
- General fear of AI.
- (Quick to make, difficult to test.)

Hoe test je AI

- Do not test outcomes, test patterns.
- Test your data.
- Test for robustness.
- Test for interests.
- Let people watch the process.
- Read the guidelines.