

ICT Research Methods for Machine Learning Engineering

apr 9, 2020 | Fontys Hogeschool ICT, Medewerker, PRO ICT, PRO Techniek | 0 Reacties




*"As an ICT student or professional, you need to solve all kind of ICT challenges. Answering the questions and tackling the problems or opportunities of your ICT project requires practical research and often a combination of various ICT research methods. The toolkit on this website offers you a set of possible research methods and a **framework** to select the appropriate (combination of) methods." (ictresearchmethods.nl)*

The Design Oriented Triangulation (DOT) Framework

At Fontys Applied University for ICT (Fontys ICT) we use the Design Oriented Triangulation framework to teach our ICT engineers how to answer the practical research questions in their ICT projects. The above mentioned website explains the DOT framework and a set of practical research methods placed within the framework. We expect from our students that they identify the questions, select preferably multiple methods to search for answers (triangulation), report on the results they find using the methods and draw a final conclusion answering the question.

"As a bachelor of ICT, your research aims at creating an ICT product which fits its needs (in this context an ICT product can be a software product, or an ICT design or advise/report). The

research is focused on the product, and not per se on creating new knowledge which is the aim in most scientific research. ([ictresearchmethods.nl](https://fontysblog.nl/ict-research-methods-for-machine-learning-engineering/))”



Library	Field	Lab	Showroom	Workshop	Extra
Available product analysis	Document analysis	A/B testing	Benchmark test	Brainstorm	Joker
Best good and bad practices	Domain modelling	Component test	Ethical check	Business case exploration	
Community research	Explore user requirements	Computer simulation	Guideline conformity analysis	Code review	
Competitive analysis	Focus group	Data analytics	Peer review	Decomposition	
Design pattern research	Interview	Hardware validation	Pitch	Gap analysis	
Expert interview	Observation	Non-functional test	Product review	IT architecture sketching	
Literature study	Problem analysis	Security test	Static program analysis	Multi-criteria decision making	
SWOT analysis	Stakeholder analysis	System test		Prototyping	
	Survey	Unit test		Requirements prioritization	
	Task analysis	Usability testing		Root cause analysis	
	Exploratory data analysis	Data quality check			
		Model validation			
		Model evaluation			

Fig 1. ICT research methods in the DOT framework (new ones for machine learning in yellow)

What the DOT framework calls “research methods” are methods that have been long considered part of the standard toolbox of the ICT engineer:

- “Field” methods to explore the application context, e.g. engineer user requirements;
- “Library” methods to explore what is already done and what guidelines and theories exist that could help you further your design, e.g. relevant design patterns, frameworks, libraries, tools;
- “Workshop” methods to design and implement the product (prototype) based on the results of Field and Library methods;
- “Lab” methods to test what has been implemented;
- “Showroom” methods to validate the quality and value of the product.

Nevertheless, from an educational perspective the DOT framework gives us a way of unifying the way of working for all ICT students (not only at Fontys ICT). It helps us framing the graduate project of our students as practical research projects in a uniform way.

Machine Learning (ML) Projects

From an engineering perspective an ML project is a software system that has one or more components in it that learn from data. This entails the collection and pre-processing of data, the training of an ML model, the deployment of the trained model to perform inference and the software engineering of the encompassing software system that sends new input data to the model to get answers.

In a previous [post on ML projects](#) I explained that more and more graduation projects for our ICT students have a machine learning component in them. I also argued why this is different from traditional rule-based software engineering and I identified eight challenges for engineering machine learning applications:

1. Data requirements engineering including data visualizations
2. ML components are more difficult to handle as distinct modules
3. Design of the ML component through algorithm selection and tuning
4. Break up the ML development in increments
5. Data and model management for the current and future projects
6. Find ML models that can be reused for your application
7. Validation of ML applications in absence of a specification to test against
8. Explainability of ML models is needed for debugging.

In my current research project I am collecting tools and methods to address those challenges. I published a [post on software testing for ML applications](#) aimed at practitioners applying this in their project (challenge 7 and 8 above). But I have found many more tools and methods for ML projects and I am adding new ones each week. Note that in my research I focus on supervised machine learning for predictive analytics, i.e. the use of labeled training data to train a model that is able to accurately predict labels for unseen data.

New ICT Research Methods for ML Projects

The current set of research methods on [ictresearchmethods.nl](https://fontysresearchmethods.nl) contains only one research method that refers to machine learning: the “Data analytics” method in the “Lab” strategy. This does not reflect the way of working in ML projects, where Data Analytics is not a method to answer one question but a method to fulfill the main goal of the project. For ML projects, the Data Analytics method should be divided in several smaller steps, each becoming a method of its own. In other words, we should treat the Data Analytics (or more appropriate ML engineering) process in the same way the software engineering process is treated in the framework.

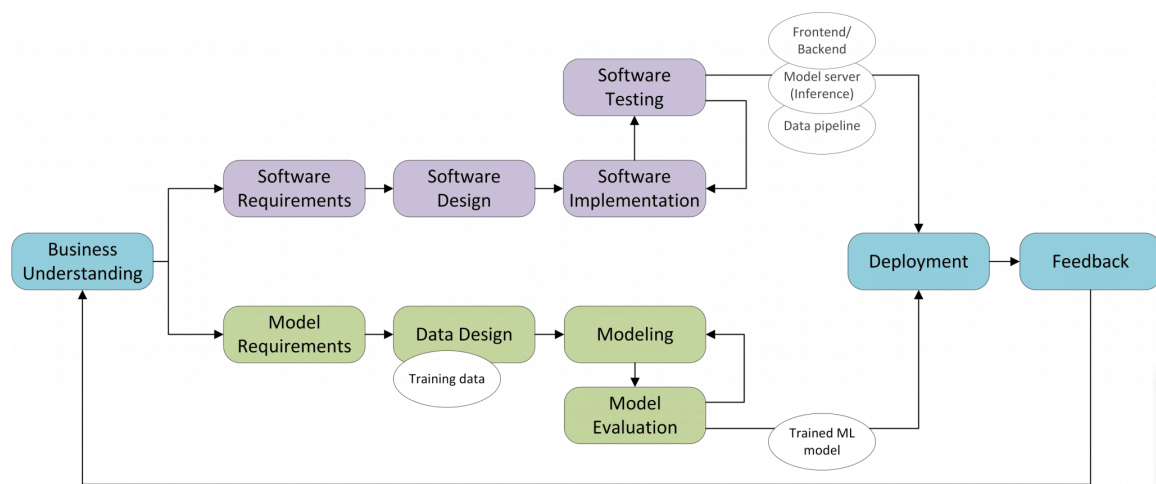


Fig 2. Steps in an ML project

For that we can use the highly schematic picture adapted from my [previous post on ML projects](#), see Figure 2. In green, it shows us the steps (high-level, derived from CRISP-DM) that should be done in the machine learning part of the project. For the research methods this means the Data Analytics method should be replaced by several separate methods:

- **Data collection.** Based on the model requirements (what type of data?) and the business understanding (which content should be in the data?) we should collect the data that is needed to train the ML model.
- **Exploratory Data Analysis.** Instead of requirements we have input data. Instead of interviewing users to collect requirements we should explore the given data to learn what we can do with it. This is called [Exploratory Data Analysis](#).
- **Data preparation.** Once we understand the data, we should transform the data such that it can be used for training an ML model.
- **Data quality check.** Next to testing the software we should also test the data. It is well known that with wrong input data, the model will also produce wrong answers.
- **ML model training.** The way to approach the training of ML models is very specific; algorithm selection and hyperparameter tuning are part of it.
- **Model validation.** Next to testing software and data you also need to test the trained model.
- **Model evaluation.** Translate the ML model results to communicate and validate them with end users (e.g. through data visualization).

These seven methods also are mentioned in the Data Analytics method as you can see in Fig 3. Data collection, data preparation and ML model training are engineering steps that do not qualify as ICT research methods. According to our experiences with ML projects the other four methods require a “card” of their own.

Data analytics

[Contents \[show\]](#)

Why?

Gain insights by measuring and analysing data. Researching a dataset can give you useful quantitative information about the topic of interest.

How?

Collect data that is relevant for your area of research and analyse it. Split your dataset into a training set and a test dataset. Find an algorithm that works with the training data and check whether it is reliable with the test data.

Ingredients

- A data collection plan.
- Analysis tooling (e.g. statistical tooling or machine learning algorithms).
- A critical eye on the validity of your data and your conclusions.
- Comprehensive data visualisations

In practice

Applied data science is now done in many fields. For example, it is used in the business domain to predict customer behaviour.

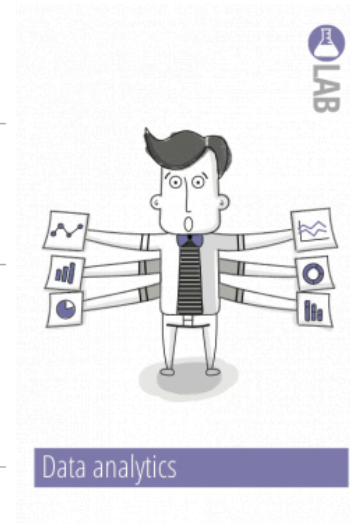


Fig 3. Data Analytics Card

Existing ICT Research Methods for ML Projects

In the remainder of this post I will briefly discuss each of the existing research methods and how they apply to ML projects. The methods are organized by strategy. In the discussion I will give pointers to relevant tools or literature for ML projects.

Library

Available product analysis Reuse of models is an important topic for machine learning projects. This can be through an API or by downloading the model code and implementing it in your solution. Reuse of (open) data is also worth to investigate.

Best good and bad practices Very important for machine learning projects. Sources of good practices are usually big companies like Microsoft that already have a track record in ML projects. Note that ML engineering is a relatively new discipline so best practices are still emerging. It is also a hype so you might be overwhelmed with what's out there.

Community research Main source of information for solving any technical issues you run into during the implementation of your ML model.

Competitive Analysis Might be necessary to identify the problem you are trying to solve with your machine learning application. What is the business goal for the project?

Design pattern research Since ML engineering is quite new, there is limited knowledge on design patterns. A good overview is provided by [Washizaki et al.](#) We also see more

developments going towards layered architectures for ML systems, like the **TensorLayer library**.

Expert interview As a machine learning engineer you will probably work with data scientists who come up with the advanced models that you implement.

Literature study You probably need this to identify possible ML algorithms for your problem domain. E.g. research on “anomaly detection in time series” or “object detection in images”.

SWOT analysis See competitive analysis.

Field

Document analysis For ML projects it is most important to understand the data you will be working with. Any document explaining the data or the processes that produce the data could aid in this understanding. You also need to understand the purpose of your predictive model. In what way will the predictions be used to support a certain workflow or process? Documentation describing the workflow or process could aid in this. Furthermore documentation about the existing IT environment in which your ML application/module needs to operate is a good source to start from.

Domain modelling Domain modelling can help in understanding the data you will be working with.

Explore user requirements Although you still need to define user requirements for your end solution (the front-end that serves your model predictions to an end-user), you also need to focus on the data requirements: which training data is needed to train a good predictive model for unseen data? For this you also need to discuss with the stakeholders in an iterative process, because end users or domain experts are the ones that understand the data and can help you find incorrect or missing data.

Note: I propose to add a new method “Exploratory data analysis” for exploring data requirements.

Focus group With ML solutions the system is self-learning. For certain applications it is important to make the predictions or decisions of this type of model explainable. A focus group might help you discover if your solution will have trust-issues for end users.

Interview Next to end user and other stakeholders you probably also need to interview IT experts or data scientists to get expert knowledge for your project.

Observation This is a good way to find out which steps in a workflow would benefit from automated predictions or decision support. Ask people which rules they are using in their head to complete their tasks/steps, which data they use and if they in any way need to pre-process the data.

Problem analysis Also for ML projects there is always a problem you are trying to solve. Understanding the problem/opportunity helps in deciding when your model is “good

enough” and with all other decisions you have to make during the ML project.

Stakeholder analysis To get a good understanding of your project you need to get input from all people involved or influenced by the project outcome. You will usually only deliver a prototype but do not forget to include roles like maintenance/devops who might need to run your solution in production in the future.

Survey You might use surveys to reach out to a larger group of people at the same time (compared to interview).

Task analysis You should focus on the data used/processed and any steps that could benefit from decision support or automated predictions. What are the rules currently used for making the decision or prediction?

Lab

A/B testing A good way to discover which version of the model delivers more value to the end user. You need to incorporate logging or diagnostics that helps you decide which model “works better”.

Component test ML systems are difficult to divide into components so you need to come up with a clever way of doing this. ML components typically also interface through the data pipeline or shared data, so be aware of any adverse effects of changing one components behaviour on other components that use its output data.

Computer simulation Simulation models can be used to provide predictions to the end user or to optimize processes. Simulation models (a digital twin) are also used in situations where it is difficult to collect data from physical systems. The digital twin is used to collect input data and to test how the system responds to predicted output data. The use of digital twins is typical for training reinforcement learning models.

Note: for ML projects this is not a Lab method, but a Workshop method.

Data analytics For ML projects this is not merely a Lab method. Its components “data collection”, “apply ML algorithms”, “data validation” and “ML model validation” merit separate methods in the framework.

Hardware validation If your ML solution needs to run on hardware components this might be part of your project to validate the component first.

Non-functional test The paper by [Zhang et al.](#) provides a good overview of the properties to be tested for ML systems: correctness, overfitting degree, fairness, interpretability, robustness, security, data privacy, and efficiency. The paper also sums up a literature overview of the methods to test them. I made a practical translation of that in my [post on testing ML applications](#).

Security test Also for ML systems you need to find and prioritise vulnerabilities and determine their impact on the confidentiality, integrity and availability of information. Privacy issues are involved if the system processes personal data.

System test Since the system is self-learning (you did not program the rules yourself) it might be difficult to assess if the system is behaving as required. You need to think about how you will test this on beforehand, see my [post on testing ML applications](#) for pointers. Usually you will keep aside part of your data for the final testing.

Unit test See component test.

Usability testing It is also important for ML solutions to test how well the end user is supported in the task the user needs to perform. Make sure you have a proper front-end (UI) through which the user can interact with the ML model and its outcome.

Note: I propose to add separate methods for testing data and model: "Data quality check", "Model validation" and "Model evaluation". See also my [post on testing ML applications](#) for pointers on these topics.

Showroom

Benchmark test "Benchmark tests are regularly used to test pattern recognition software. If a standard set of data is recognised with the software, the results can be compared to that of other software." (quote from [ictresearchmethods.nl](#), method Benchmark Test) An example of this is the [MNIST dataset](#) with handwritten digits that also shows test error rates for many different methods.

Ethical check Ethical checks are even more important for ML solutions because you do not design the rules yourself, but let the system learn the rules from data. If the data is biased, this can result in unintended behaviour. You need a way to insure that the behaviour of the system stays within ethical boundaries. You must also make sure that the system is not learning something that invades people's privacy. The [Technology Impact Cycle Tool](#) provides a practical translation of several ethical considerations into a questionnaire and might help for your project as well.

Guideline conformity analysis The guidelines that apply to software systems of course also apply to ML software systems. Since 2017 there is a group at ISO ([ISO/IEC JTC 1/SC 42](#)) that works on standardization in the area of Artificial Intelligence.

Peer review Having your work reviewed by peers is always a good idea. ML code is difficult to review because most ML algorithms are black boxes. It might be more valuable to organize a walkthrough of your ML experiments where you talk your peers through your way of thinking in designing the ML model. How did you come up with the final algorithm and its hyper parameters?

Pitch It is a good idea to also think about the business proposition or opportunity you see for your ML solution. Knowing the added value of your solution helps you make decisions during your engineering process.

Product review Because of the experimentation required for engineering ML models, you will probably be working in an iterative or agile way. It is good practice to deliver a working model/product at the end of each iteration and have it reviewed by the client or

users. If it is a model you deliver, you need to think of a good way for others to review or demonstrate it.

Static program analysis You should also run code quality checkers on your ML software. However, since the most important code (ML library calls) behaves as a black box, you need additional quality checks as well.

Workshop

Brainstorm Since the engineering of ML solutions is highly experimental (trying out algorithms and their tuning) it is recommended to use brainstorming to get the input of others in those experiments. What to try next? How to improve our model score?

Business case exploration It might be necessary to compare a scenario with ML to a scenario without ML. Is it worth the effort or investment to start an ML project?

Code review The most important code (ML library calls) behaves as a black box. To get the most out of your code reviews it is recommended you chose a talk through or pair programming approach. See the [blog of David Tan](#) for some examples of recommended coding practices.

Decomposition Decomposition of ML components is a known difficult problem. Still, you must be able to break your entire ML solution into smaller components. In engineering, the concept of pipelines is used to break the ML workflow into smaller steps, with each component in the pipeline being responsible for one step in the workflow.

Gap analysis Gap analysis is another way to compare a scenario with ML to a scenario without ML. Where the business case exploration serves as an economical comparison, the gap analysis helps in understanding the design goals of your solution.

IT architecture sketching Training ML solutions usually involves a cloud infrastructure to have enough processing power. In some projects you also need to think about the IT architecture needed to deploy, run and maintain the ML solution.

Multi-criteria decision making An ML project may involve choice about tools, libraries, algorithms. It is a good idea to make these decisions visible by comparing alternatives against criteria.

Prototyping This is the main goal of the ML ICT project: create a working prototype of your ML solution. For ML prototype this involves some specific techniques like feature engineering, cross-validation, hyper parameter tuning, grid search, data quality checking, data preparation.

Requirements prioritization Both data requirements and user requirements need to be prioritized. In ML projects you typically work in an agile way so this prioritization is then done through sprint backlog planning. It is good practice to first develop a working

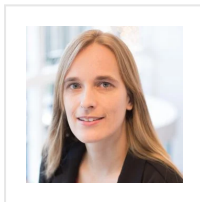
product with a “dumb” model and minimal dataset and then gradually improve the model complexity and the quality of the input data.

Root cause analysis If the goal of your ML solution is to solve a problem in the current situation, you first need to determine the root cause of the problem before you can design the proper solution. Root cause analysis can also be used for problems that arise during your ML project.

Conclusion

In this post I have discussed the Design Oriented Triangulation (DOT) framework for machine learning projects. Although the DOT framework is only used in an educational setting (ICT research methods for practical research of ICT students) my discussion provides valuable insights for practitioners as well. It is an overview of tools, methods and best practices to be used in ML projects. It provides the ICT engineer with pointers of how the tools and methods change when applying them to machine learning projects.

♥ Vind ik leuk



Over Petra Heck

Petra werkt sinds 2002 in de ICT, begonnen als software engineer, daarna kwaliteitsconsultant en nu docent Software Engineering. Petra is gepromoveerd (kwaliteit van agile requirements) en doet sinds februari 2019 onderzoek naar Applied Data Science en Software Engineering. Petra geeft regelmatig lezingen en is auteur van diverse publicaties waaronder het boek "Succes met de requirements".

[Mail](#) | [LinkedIn](#) | [More Posts\(8\)](#)

<input type="text"/>	Zoeken
----------------------	--------

Favoriete posts

De droom voor Fontys uit een verscheurde Linda (1)

Abonneer je op al onze Fontysblogs!



Your email:

SUBSCRIBE



Fontys Hogescholen