

## Week 1

### Video Transcripts

#### Video 1: Introduction to the AI Design Process

In this module, we will learn about four activities required to design an AI product. We will describe each of these four activities and illustrate their importance in the design process by using examples of different AI technologies with a focus on Natural Language Processing. Before we dive in, let me give you two reasons why the design process in AI is so important.

The first reason is because of the rapid evolution of AI possibilities. This means that finding practical applications almost always requires some form of innovation. Indeed, it is very hard to copy an AI application, and they are almost always unique. This is very much unlike in other areas where you can do as your neighbor and practically get the same car, clothes, phone, tennis racket, education, and even house. In AI, copying what others do without some design work will probably result in sub-optimal outcomes.

A second reason, co-founding with the first, is the importance of AI complementary assets. Very often it is not that AI in itself provides value. What does provide value is the combination of AI with changes in business processes. In some cases where you need a piece of AI that does not exist such as a predictive model unique to your company or a specific use of computer vision to distinguish yourself from the competition, one has to design a deployment process where the organization will keep improving the technology by feeding the right training data to the machine learning algorithms and at the same time will be adapting their business processes and products to benefit from such gradual improvements. Thus, one has to design AI products with a vision of how the organization will adapt the technologies deployed.

I suggest that before you continue, you stop for a few minutes and identify some AI products you would like to design. For each of these design ambitions, keep a log throughout the course where you identify how "what" you're learning relates to each of them. By the end of this module, you will be able to organize the design effort into four activities. By the end of the course, the objective is to prepare you for many successful AI product design efforts.

## Video 2: The First Stage of the AI Design Process

We will now review the four stages of the design process, starting with the first one. I will use a certain logic to explain the stages one after the other, to help you understand what is needed to design an AI product. However, each stage is an activity in itself. And all can really be done simultaneously or in a different order than the one I will present them in.

In this first stage, we have to identify a behavior we expect artificial intelligence will do. Basically, the AI without the "artificial", i.e., let's just think about intelligence. The intelligence that we will aim to use eventually in an artificial form. There are two challenging choices that need to be resolved in this first stage. Performance metrics and scope.

I will now introduce these two challenging choices and show some examples on how to address them. I'd say one of the biggest challenges, if not the biggest challenge in the design process is to clearly spell out what are the target intelligence performance metrics that we want to implement with artificial intelligence? And this is difficult because what AI can do is so rapidly evolving. That is, the performance frontier in our chosen domain is most likely evolving rapidly.

An easy illustration of the speed of change of the performance frontier can be seen very clearly in what happened with computer vision in the first decade of the century. You will see on this chart how that recognition rate on a big dataset of images called ImageNet evolved over time. For benchmarking purposes, the human error rate on this classification task is 5% because the images are challenging and difficult. This means that if your choice is to set yourself a performance metric of 5%, then you want to implement an AI that is as good as humans in this task.

And in only five years, as you can see in the chart, from 2010 to 2015, recognition rates went from very bad to superhuman performance. In 2010, the state of the art in artificial intelligence had an error rate of 25%. That is, one in four images in the dataset were incorrectly labeled, far away from the 5% human error rate. However, in the subsequent five years, AI improved so rapidly, that it surpassed human performance. That is what we call superior human behavior. And imagine what this five-year evolution meant for business models based on computer vision that started in 2010. They had to forecast this evolution and take it into account into their plan. A second and related challenging choice, the second one of this first stage, is to spell out what is the scope of this superior behavior that we are expecting to implement?

For example, in the case of self-driving cars, these classification tasks may give us a hint that it's possible to locate all traffic signals in the road just with computer vision. And, in fact, those performance levels achieved beyond 2015 are consistent with the rapid advancements of self-driving cars and the associated technologies. But there may be unforeseen challenges between existing benchmarks like ImageNet, and what we're trying to achieve in our target domain like self-driving cars.

In fact, there are a number of differences between the image classification task and what self-driving cars have to do such as the fact that self-driving cars process video sequences and not static images, and therefore have more information, and more information to process. Or the fact that some traffic signals may be hidden. Or the error rate that may be tolerated is definitely not 5%.

So, in this first stage, the more precise you can be for what is important that the artificial intelligence does, the better. But it's OK not to be extremely specific until you've gone through the next stages at least once. Especially if this is the first time, you're thinking about it. In some cases, like in the self-driving case, the models chosen, and the approaches chosen, the selections done may restrict what the self-driving option is implemented. Instead of traffic signals, you may choose to focus on finding pedestrians or bicycles. And then you may decide that to distinguish between them and inanimate objects, it's a good idea to use infrared cameras that help you identify warm objects like people. And in some cases, those warm objects or the infrared signals are a complement that can work together with computer vision, iron out some of the issues, and help you bring down that 5% error rate on the ImageNet case for human.

Therefore, what we need to do in this first stage is to address these two challenging choices. First, the performance metric choice. Understand how the performance frontier may be evolving in our chosen domain, so we can send targets for the AI design. And second, the scope challenge. Understand what is the scope of what we're asking AI to achieve. What is the intelligence we need in our application? The four stages in the design process may have to be revisited more than once as I hinted before.

So, if this is the beginning of your design process, it's OK to be a bit generic and come back after you've done a first iteration of stages two, three, and four. The second time around you may be better equipped to address these two choices, metrics, and scope. It is also possible that the second time around you pivot your original thinking based on finding from your first iteration, like many self-driving companies did, lowering their standards into finding specific solutions like detecting pedestrians or bicycles sometimes in restricted environments, like in urban environments where many of the accidents occur.

### Video 3: A Review of the Four Stages Centered on NLP

Let's now move away from computer vision and explore as an example another area that is also experiencing a lot of progress: natural language processing. The artificial intelligence that we may want to include in our design maybe related to one or more natural language tasks, just like what happened with computer vision.

In the specific case of natural language, we may be interested in translating product documentation, or maybe legal documents. Annotating news for executive readership, or for scholarly research, or for health clinical trials. Describe in words a given scene or data spreadsheet. Summarize a long document into a few sentences. Fill forms of specific customer requests. Answer questions automatically in a sort of chat box style fashion. Maintain a dialog to entertain people although this one is still very, very challenging. Determine whether reviews of a product are positive or negative, to get an idea on the sentiment of a market for some of your products; or what is the sentiment not of customers but of employees towards the company's brands, maybe based on Instagram comments or other information that employees may be posting.

The field of natural language has seen a lot of progress towards some of these and other tasks. And some basic required functions that are needed, such as what's called named-entity recognition (NER) or positional tagging, are practically solved like beyond human performer. And we're reaching human level performance in many of these tasks and even better. There is excellent progress, also in more elaborate tasks, such as the sentiment analysis, I was mentioning before, or coreference resolution i.e., identifying expressions referring to a given entity in a text, or word sense disambiguation and parsing and many others. The combination of all this progress has made services like machine translation progress immensely.

What is still really hard are things that relate to story understanding, as Patrick Winston used to call it, or longitudinal conversations, such as having a continuous dialogue, including question, and answering, as a five-year-old would be able to do is still very difficult. The state-of-the-art in NLP includes advances such as transformers, which can have very general- purpose applications.

An example of this is GPT-3, which in its time was the biggest investment example in terms of effort and design, and learning time, which was trained on all the written texts available. Think about it, anything that humans have written was given to the system. It became the largest model in terms of parameters with over 50 billion of them. That's more than inhabitants on the planet. Requiring just on electricity to power the computers more than \$5 million to train the model. And you will do some exercising this using it as part of the class.

In the picture, you can see how it completes a number of phrases. And again, it's the same system, it's a toolkit. You give it a phrase like, for example, a number of words, and it actually completes the sentence. You can see there the example of the shopping list. You have a number of items in your shopping list, and it completes the fourth item. It says, I add milk, and then it completes a whole story.

Other examples, you can start a piece of news and it creates like fake news that sound pretty real and very often indistinguishable from human written text. And that's where GPT-3 is at. And you can explore all the uses. I tried it, for example, to design a new class. I said, I'm going to design a class on Introduction to Computer Science for freshmen students. And it completed a whole design. It made up schedules. It made up policy, grading policy, exams, etcetera. So hopefully you'll enjoy looking at it.

## Video 4: The Second Stage of the AI Design Process

Let's now talk about the second stage that is to find the business process that AI can support. To find such a business process, there are two key issues that need to be addressed, the strategic one that involves deciding how will AI play out in our long-term sustainable advantage, and the operational one that is specifying the business process where AI will intervene in setting performance targets for such process, including not just AI but other collateral assets.

Let's start with the first of the two, the strategic AI choice. Here, we need to decide how we will use AI to compete in the marketplace. That is, what is the role that we want AI to play in our design process? One way to think about this is to use the Delta model developed by Professor Hax at MIT Sloan which postulates that there are three ways to compete. Let's now review the three of them.

The first strategy is to be a best product player. In the case of AI, this means having the best technology possible. For example, the best fingerprint recognition software. Anyone interested in the applications that can be based on fingerprint recognition, we want to use your product, if they can afford it. Another strategy, a second one according to a Delta model, is to be a full customer solutions player.

In the case of AI, this means providing a product that incorporates all AI and all the associated features that will make it a useful product or service. For example, a security and access control solution for buildings that maybe your company already has, that now incorporates fingerprint recognition software and other functionalities required by customers such as locks, intrusion alert mechanisms, connections with the police, 24X7 recovery services, mobile app unlocking, etc. You may not have the best fingerprint AI in the world, but you're offering a service that is useful to a certain segment of customers that therefore will buy it. A third strategy, and the last one of the Delta model is network externalities.

Here, the focus is on building the largest user base possible in a way that results in user getting more benefits as the size of the database increases. For example, you may focus on building a nationwide database of fingerprints so that police can quickly identify people in criminal scenes. The more municipalities and states that participate, the more likely it is that the database is useful. You may need AI for fingerprint recognition, but you don't need to have the best one, and you don't need to provide a full solution to the police.

Most self-driving efforts, like the ones we discussed when talking about the first stage, are focused on full customer solutions because the use of AI is closely related to the design of the full product. In fact, most brands have different flavors of how they use AI.

Before we move to the second choice in the second stage, let's use another computer vision example to explore stage one, metric, and scope, that we covered in the earlier videos and this first part of the second on that is the strategic one. Imagine that instead of self-driving cars, you're thinking about the service that automatically captions images and that you want to offer something more elaborate than what is currently available on the web. Take, for example, the image on the screen.

Current state of the art services will allow you to identify that this is an image of people in a room in contrast to what traffic or a nature scene, however AI is not yet developed to a point where it can identify President Obama is playing a joke while everybody else is having a relaxed attitude. Associating a story to an image is something that AI seems far from achieving at human performance levels. Whether an image can be cheerful or not in general is something that we may also be far from achieving.

This means that you will need to address scoping challenge by somehow narrowing the requirements so that the AI can produce results consistent with what you set out to achieve. In general, when you hit an AI frontier like in this case, your creative juices should start flowing, and it's worth digging deeper into specifics, understanding that the frontier will help you in scoping the intelligence that you need to automate.

For example, AI may not be able to create general story captions, but if you want a service for a newspaper, perhaps it can extract the relevant information from the associated text to describe the picture with a specific genre and with a small phrase. Or maybe you want to translate newspaper picture captions into different languages which moves you completely away from your vision and into the realm of machine translation that we've also talked briefly about. In both cases, you may be able to produce the best product, something that all newspapers can use, so the first of the strategies we discussed on the Delta model.

A full customer solution, i.e., to integrate the solution into a specific content management system than maybe your company operates or that your newspaper company has. And also, the third one. You may create network externalities if you can produce an open system that all newspapers use in a way that you can capture how editors modify AI suggestions so you can continuously improve the service. Still on this computer vision captioning example, if you want a generic service and you cannot produce this generating service that captions everything like humans, you may be able to focus on a specific type of captioning and you may be able to tell what is the sentiment of people in an image so that you can add sentiment to a general captioning software.

GPT-3 is an example of natural language processing, best product strategy to switch from computer vision to NLP. The declared goal of the company that produces it, OpenAI, is to create a toolkit so that companies can adapt the model to various tasks. The model is so powerful that its creators even warned about the possibility of abusing it for malicious goals such as generated fake news as one of the applications that we saw in the earlier videos. The text produced is so realistic, it makes it very hard for humans to distinguish between human text and GPT text, as you'll experience in one of the exercises given to you.

Let's now move to the second choice in this second stage which is operational. What is the business process that will benefit from AI, and what are sensible improvement targets for that process, and what are things that you need to address within the process, not just in AI? The idea here is to focus on the process that will be impacted by AI so that it can give the engineers adequate information on what is expected of the AI implementation. We need to define a business process and how AI will improve its performance targets.

In the next stage, that is in the third stage, we will be focusing on choosing their specific technology and what AI can be introduced based on the performance targets that we've set. And, hopefully, there will be such AI and a cost we can afford. So, let me give you some examples of operational targets that we can set in this second stage in the case of natural language processing.

If you apply it to answering questions in a call center, you want to lower uncompleted calls by 80% in a call center at the same cost so that the responses that the system give have improved and there's less issues with those answers. Or you may want to lower legal translation costs by 80%, maybe because you produce a first version of the translation and then the lawyers only have to review it and they focus on that tricky places. Or you may want to add voice commands to a webpage. Very few people talk to webpages, but you may want to add voice recognition in the webpage so that you can navigate with voice. Or you may want to create a shopping list assistant skill for, you know, an Alexa or a Google device or another one or your own. Or you may want to create a sentiment analysis toolkit, sort of like a bit like GPT-3 but for sentiment analysis. You can create full personal assistant Alexa with improved skills, and therefore your target is an existing product that you're competing against to. Or, you know, to be even more ambitious, why not improve on GPT-3?

But it's important to stress that these targets that we put on the process are not all that's needed in connection with this AI process we're designing. For example, when we need to seek authorization from the user, which means a new consent form that needs to be worked on, or we may have to renegotiate insurance terms. In this stage, we need to define well the process and make sure we address all of the required collateral assets required. Sometimes, they call them the complementary assets to the AI technology we'll be using. And often, these investments based on research done by Professor Brian Nielsen at MIT Sloan, they require sometimes 90% of the total investment dollars. So, they're very, very important.

In summary, what we need to do in the second stage is to address these two challenging choices. First, the strategic use of AI as a best product, full customer solution or as creating network externalities. And second, the operational description of a process, including non-AI requirements and specific process performance metrics where AI will help. That is the AI without the AI. Let's now move to the third stage.



## Video 5: The Third Stage of the AI Design Process

So far, we've made it through stages one and two. In stage one, we focus on two key choices, AI metrics and scope. In stage two, we also focused on two choices, the strategic role AI would play, and the operation targets we would set for the business activities when AI was going to play a role. In other words, before you start with stage three, you have already identified an intelligent behavior you'd like to implement using artificial intelligence, and you also have a business objective that you would like to achieve. The latter includes some business activities where artificial intelligence will be used.

In this third stage, focused on AI technology choices, there are also two key decisions to be made. This is a good mnemotechnic for those that like them. Two choices in each of the first three stages. Well, and what about the fourth one? What do you think? Exactly. Also, in the fourth stage we will have two choices. Four stages, two choices in each. Yes, that's eight choices in total. Learning science tells us that this type of coincidences are great anchors for learning. I hope it helps you retain the content.

As an AI product designer, you have to make eight choices. Eight is also a key number in dancing. Learning science also tells us that if you search on your own why dancing is mostly based on eight step sequences, that will help you retain this important number in AI. Learning science tells us that it must be you making the effort, so I won't reveal anything more about dancing. It's another coincidence that probably will help you. Making connections in your brain between different areas helps you solidify the learning and the versatility across domains. So, let's go back to AI which is really why we're all here.

On the third stage, the first choice of the two involved centers on selecting the right intellectual property approach, and the second one on picking the right data strategy. Let's now review these two choices, IP around the technology and data entered. So, now, starting with IP or intellectual property or the choice of the technology that you'll use for AI, thinking about stages one and two, they have provided you with the right specifications of what artificial intelligence technology will add to your business strategy. Now, you need to be more concrete and pick a specific artificial intelligence technology that you can incorporate in your product.

This selection is very difficult because AI is a general technology, and there are many choices evermore. We're talking about thousands if not tens of thousands. To put the number of technology options in perspective, know that up until 2012, the number of patents related to AI was not very large, and it was not growing significantly. However, since then, the number has skyrocketed, growing year after year, and only in the U.S. there are thousands of patents awarded every year. This makes the life of AI product designers very exciting because there are always new things. But also, very risky, and tricky because one may pick something that is just obsolete in a few months.

Confounding with a growing myriad of choices, there is the lack of off the shelf alternatives. The good news is that there are so many new opportunities for AI that chances are you'll be able to patent what you design. And this should also be part of your IP approach. This course is not going to teach you how to set up a patent, but if your use of AI is novel, useful, and nonobvious, I strongly encourage you to consider patenting. The rest of this course will help you get a better understanding of what these technology choices may be.



## Video 6: The Third Stage—Data Strategy for the FAANGs (Part 1 of 3): Facebook

You will learn in the next modules what are the specific advantages and disadvantages of each machine learning approach and what roles AI may play in human-computer interaction, in designing new Superminds, and in manufacturing robotics. What all of them have in common is one thing, data.

In this third stage, the second decision you have to take is what data strategy you're going to follow. In fact, there is a close connection between the data you have and the algorithms you can use with it. The algorithms are related to your IP and the data to the data strategy. And one of the critical issues on data is how it's labeled. This labeling is in fact data about data, and it's why it is called metadata, and it includes such things, at a minimum, as date, time, collection mechanism, and description of its content. If your data is not properly tagged or if you don't have enough metadata associated with it, you'll be restricted to what you can do.

Perhaps even only unsupervised learning. In many ways, though, the data strategy is also disconnected from the machine learning algorithm. The more data and metadata you can have, the more options you'll have. Perhaps you have data for which no AI algorithm has been already developed, but this may change eventually. This happened, for example, with a picture libraries on the phones. Now that we have face recognition, they are a lot more valuable because they can be organized automatically by person. So, you can automatically organize photographic memories by contact. It also happened with text. Most of text written by humankind was never used to AI until recently GPT-3 read everything that was available. And in doing so, it was able to give new use to the collection of text that very few people read.

Who knows? One day AI may read scientific papers and invent new theories and design its own experiments. The opposite feedback force also exists. If you have AI technology that automatically adds metadata to your existing data or that generates new data, you'll have more data upon which to build further AI algorithms. You may even be able to sell it as a business. This is the basis of some of the most successful AI players. Google, in fact, sells your data for advertising purposes. It keeps tagging data and lets others decide how to use it. In fact, the big AI players in the world all have very sound data strategies.

The so-called FAANGs, which stands for Facebook, Apple, Amazon, Netflix, and Google, now Alphabet, have a data strategy that gives them network externalities, allowing them to really test any of the machine learning approaches you'll be exposed to in module two. The data approach of the FAANGs share many things in common, and the end result is an advantage thanks to the data they have.

That's why a lot of people say data is king or data is gold. Let's now see these similarities a bit more in depth. And hopefully, you'll learn from that and get inspired to develop your own data strategy. I'll use a framework, as you can see on the screen, to help you understand the sources of this superior long-term sustainable advantage that data gives. The value from the data, according to this framework, comes from three interrelated forces that fit into each other. Companies that can make their AI strategy accommodate these three forces will gain a natural long-term sustainable advantage thanks to their data superiority.

Externalities is the first of these three interrelated forces. We've already talked about this when covering stage two as a possible strategy leveraging AI. Take Facebook for example. For a given user, the value of a social network is based on the amount of users the network has. If two networks have similar services, but Facebook has 95% of the "friends," quote-unquote, of a given user, and the other one only 1%, that user is definitely more likely to pivot towards Facebook, everything else being equal, because it is the one that has more of its social circle.

Network externalities is not a concept restricted to AI, and it operates similarly in other domains like with the phone network. What would be the value of a phone if you could not talk to anyone? The more users that have access to a phone, the more valuable it is. In the case of Facebook, this also means that it is the network with the most data related to social networks and therefore the one that can better test artificial intelligence algorithms related to advertising. That explains why Facebook has been so quickly at purchasing other big social networks like WhatsApp or Instagram. For both of these, the possibility of integrating their services with each other meant that the collective value was larger for everyone.

In summary, network externalities has three components that pivot users to the largest of the various options in the market because the larger the community, the more value per user it can deliver. And because the larger the community, the more value the asset has for operators that target the users of the network, such as advertising companies. It is really in the interest of everyone to have one big network where all can join. This is true online where you can go anywhere with one click. It sort of also applies on ground. Who would want two Sunday markets in a small town one kilometer apart from each other, If you could have both of them be one and in the same place? From the point of view of the customers, they could go to a place and compare options instead of having to go back and forth between the two. And for the sellers of goods, they would only need to serve one location with advantages translating to key retail metrics such as out of stocks, shrinkage, operating costs, etcetera.

The second force of the network externalities is system lock-in, and it relates to how the FAANGs increase switching costs from their services. In the case of Facebook, Instagram, and WhatsApp, this means that you have all your contacts, pictures, message history. With groups, they make it super hard to change because in theory, you'd also need to change all of your contacts and at the same time to have the same experience somewhere else. It also means that you've learned how to use the application, including all of its features. You have set your privacy settings, notifications, profile picture, and other configuration options that make it hard for you to switch.

But system lock-in does not apply only to end users. It applies to the advertisers, developers, and third-party application developers. Perhaps your company has a company license or has pre-approved advertising terms with Facebook, which would require a new negotiation if you were to change. Who knows? Perhaps you have developed your own AI algorithms, like hotel reservation systems do, and that is based on a history of Facebook information. It'd be practically impossible to change all of these without significant costs. That's why it's called system lock-in. You've been locked in, your suppliers and any other provider, too.

Finally, the third interrelated force are economies of scale, which operates alongside system lock-in and network externality. As a result of the other two forces, the winning player in the network externalities race will see its revenue rise. See, for example, the advertisement revenue of Facebook between 2009 and 2019 before the COVID pandemic hit the market. You see that these revenues grew exponentially from less than a billion to tens of billions. What this means is the possibility to afford a larger R and D budget to continue to fund whatever future improvements are needed to increase the size of their user base or even to buy competitor. And more users means more data, and that means better trained AI algorithms.

## **Video 7: The Third Stage—Data Strategy for the FAANGs (Part 2 of 3): Amazon, Apple, and Netflix**

Getting to the position where you have a snowball effect like the one, we described for Facebook is not easy. In the case of the FAANGs, they all underwent brute force, large investments, including bank competitors, which provided them an edge over the competition. Let's review briefly some of the other data strategies. We started with the F in the FAANGs, let's now go for the A's. Amazon has network externalities on different fronts.

Currently Amazon.com as a retail shop, is sort of like the town market but at scale. If you include their partners, they sell hundreds of millions of product. You can get your products on their catalog; chances are you will see more of them. I'd like to talk about one aspect of their artificial intelligent program that has a lot of data sources.

The full AI program at Amazon ranges many topics including their Amazon Go automated retail stores, face recognition services, including tens of millions of faces, robotics, and more. The one I'll talk about is one of their most successful AI programs, the Echo line of smart speaker products. I'll be talking about health diagnosis using voice and how it could be incorporated into Alexa. The way this speaker product works is that when you tell them in your room, it's always listening. And when it hears a wake word such as "Alexa", it wakes up and listens for the following set of words expecting a command like "play Dire Straits" or "add cereals to my shopping list".

Some of their products have cameras too. In terms of getting data for AI intelligence, is hard to think of a better setup. The device has some network externalities, but not as much as other products. The reason is because from the user's point of view, the number of user does not matter very much as long as it plays Dire Straits when you ask for it.

The one service that smart speakers provide that requires a network is that drop-in feature where you can talk using those smart speakers. But it's not a very popular one because you can do the same thing with your phone. These lack of network externalities from the point of view of the user is what explains that Google was able to catch up in part at least in terms of market share.

As you can see on the chart. Apple AI data strategies, switching to another A, is focused on controlling the hardware market. With about 10% of laptop sales, 20% of smart phone sales, and 30% of smart watch sales, it can capture data about a lot of users. Their data store acts like a big market generating a major lock-in for users.

Unlike Facebook and Amazon, Apple can get a fairly holistic view of what a user is doing through GPS readings and their Siri “always on voice” service. Facebook, Amazon, and Apple all have network externalities and the third-party supplier level.

For example, Amazon web services has over one million developers trained to use their cloud services. This means that if you want to deploy AI applications, they have the most active programming base from the point of view of a developer, if you learn AI development on AWS, versus doing it with a residual toolkit, your employment value will be larger. Here's where the network externalities come. Once you've learned the command and how to set applications, you are then locked in, especially one to re-use the code. And this makes AWS bigger, providing Amazon with more profits to re-invest in the system, the economies of scale. Something similar happens if you develop a partner software. Software for Facebook react. Or if you write applications for Apple's IOS.

Now moving to the N, Netflix AI data strategy is based on collecting as much information as possible from the user watching behavior. By looking at what actors get more pause and rewind instances that's it a very simple metadata. Just think about it. Rewind, pause, and rewind. They can rank options for target user base.

Their artificial intelligence program uses the clicks on your remote control to enable machine learning on the hundreds of millions of subscribers they have. To have catalog composition, original productions, encoding, streaming, marketing, and advertising.

Even for picking up the roster of new production. A pause histogram can also help create a new script combining pieces of other scripts generating maximum attention within each episode. In fact, House of Cards is an example of such an approach where it's content, it's director, David Fincher, and its key actor Kevin Spacey were all the product of machine learning recommendation.

## Video 8: The Third Stage—Data Strategy for the FAANGs (Part 3 of 3): Google

Let's now look at the last of the FAANGs, Google, now Alphabet. The company initially was focused on a search engine, but quickly pivoted into a lot more. I mean, 2007, bought DoubleClick for \$3 billion in cash, and that became an integral part of their data strategy.

Let's see what Kevin O'Connor's business model, the founder of DoubleClick, was. Before DoubleClick, users of the internet could go to content sites. Let's imagine an online user, E-Joe, that you see on the diagram. That is watching content sites such as the New York Times or Yahoo. To generate revenues via advertising, content sites could partner with advertising brands like Nike. The New York Times could track users that were returning to their site, either through subscription or simply via cookies.

Cookies are an important part of the web because they facilitate tracking and personalization. They were an idea of Lou Montulli, an employee of Netscape that in 1994 suggested introducing them in browsers. They soon became a standard. When users log onto a site, cookies, which are really just a very long alphanumeric code, are sent back and forth between a browser and any given site. This allows a site to know which computer is making requests so that they continue a session even if there are hours apart between the user connecting and even if the user connects to other sites in between.

In other words, this makes it easy for newspapers to know that you are a returning customer. This allows them to build a behavioral database that helps the newspaper sell more targeted ad functionalities to advertisers. It can infer that you may purchase sneakers because you're always looking at the sport and health sections. The newspaper may strike a deal even directly with online retailers like Amazon with an ad that displays a special offer for a given sneaker on Amazon. If one had 1000 content sites and 1000 possible advertisers, that would generate over a million different contract possibilities. Perhaps the largest sites could afford the manpower to write these contracts and negotiate them.

But many of the sites were actually Mom and Pop sites without the resources for such extensive administrative handling, and at the beginning, the audience wasn't that large, nor the potential revenue justified so many contracts.

And here is where Kevin O'Connor's idea came into play. He set up a company called DoubleClick.com, based on creating standard contracts for both, content sites and advertising sites. Instead of one million contracts, now there would only be a handful of them that everybody could sign. He essentially standardized contracting terms and started a process to generate network externalities for all players.

Now, DoubleClick became able to track users across sites, making the behavioral information associated to a cookie be a lot more meaningful. It could tell what newspapers you visit, what stores you go to, and even what products you are interested in buying by tracking you across different sites.

Traditionally, advertisers in print pay newspapers for a certain reach because they cannot track performance in detail. That is, they pay a certain amount for every 1000 readers which has a cost per million, irrespective of whether the users retain anything from the ad or not or even really, they see it. But the internet allows for a different approach. AI can now help decide not only what ads to serve in a newspaper but also what news to provide the user. Through sophisticated machine learning algorithms, newspapers serve content based on user behavioral data.

Soon, Natural Language Processing will change the wording of each article to target the specific user tastes and needs, all with sophisticated ROI, return on investment metrics, governing all micro decisions that the newspaper does. Like with Netflix, AI will be all over the place in the internet media. Kevin's idea was that instead of Nike reaching a deal with the New York Times, it would strike a deal directly with DoubleClick, where it would pay a certain amount every time a user clicked on an advertising. That is advertising pricing became performance based.

At one point, DoubleClick decided to outsource the decision on what ad to serve and it created instant auctions where companies could bid to place ads. To do so, it used a dedicated network to add high bandwidth because the auctions had to be resolved very quickly. This predictive modeling companies would specialize and only bid high if they thought the user would click. The situation became more complicated with phone networks. Now, DoubleClick would get cookies from E-Joe's computer and also from E-Joe's phone. They're not cookies, but the principle is always the same, a unifying identifier that tracks a user across behavior.

DoubleClick would now auction both behaviors, the web browsing and the mobile one. One of the companies that does this type of betting on mobile advertisings is MOLOCO. Whenever you're playing with your computer and an application can serve you an ad if you do it, for example, on a mobile phone. MOLOCO decides whether to place a bet on you or not. In fact, they are involved into a billion auctions per second. I find this pretty amazing. The trend is that every time a user does something, the associated transaction string gets longer and longer and longer because more and more players get involved whenever somebody does something.

For example, once a user is identified in a website, either because you give your login information or your credit card details, information providers can join the transaction stream and exchange information with the predictive modeling companies. In certain cases, this may involve information in public registries like vehicle or house ownership or more private information like health data. DoubleClick may not be the only one, another network brokers may join the system.

In some cases, there may be intermediary players or infomediaries that mitigate between a site and DoubleClick, like, for example, Facebook does. In fact, an ad that was given a price for being the most intrusive advertisement of all times in Cannes, France was played on a regular TV. What was special about that ad is that smart speakers gave the information back to Google on which homes had the TV on. This is the first time that this could happen. Now, predictive algorithms can not only base their predictions on what you're seeing, but on ambient noise, and even on the conversations that preceded the advertisement. The amount of data that AI has at its disposition is really amazing.

The data strategy of Google is fairly comprehensive, and it does not stop here since there are many other products that can complement the behavioral database. Think of all the Nest line of product which Google bought for a billion dollars. Yes, a company that creates thermostats was sold for billions of dollars. There are many other IoT devices that can complement this like the Nest cameras or even Android phone services, or even GPS tracking. The FAANGs are not the only ones with solid data strategies. Let me give a few other examples.

Microsoft bought GPT-3 or OpenAI, largely because it had as data all the written text available. Or SAP, the big ERP software provider. In its concur system, it has computer vision to recognize receipts to automate administrative processes. They have a service that we use at MIT. I use it. That basically uses the phone camera to automatically incorporate photographed receipts into a system to track traveling expenses. Think about it. No matter what receipt in any part of the world, it collects the receipts and makes people verify that they get the amount of the receipt correctly. That is, they add metadata using their own user to guess the amount. If they, do it right, great. If they don't, they have you type it so that you help the system improve.

This is the kind of information the machine learning engineers need to improve their algorithms. This notion of improving the data categorization is critical when trying to improve AI algorithms.

## **Video 9: The Fourth Stage of the Design Process (Part 1)—Software Development**

When you arrive at the fourth stage, you already have your AI metrics and scope, your AI strategy and operational targets, and your IP and data approaches. Now it's time for action. You need to get the engineers to work on the AI algorithms, and the rest of the organization to align on the complementary assets. Tinkering with the technology is more effort than any other aspect of a technology, and gives rise to the second iceberg, the tinkering iceberg.

One usually only sees the more glamorous steps. Specification and the key architectural decisions. But the time spent on finding and fixing bugs, and on making the software work in the production environment is one order of magnitude more effort than anything else in the technical process.



Here, there are again two key choices you'll have to make. The first one has to do with your software development approach, and the second one with how you're going to deal with the AI cancers. The software development strategy has implications similar to key choices made in other types of businesses. Just to give you some intuition, for example, the choice of menu in a restaurant or the location of franchises in a retail chain or the planogram in a grocery store.

What all these choices have in common is that they have a big impact on the business outcomes, and that pivoting choices based on outcomes is important. It's sort of like the fine tuning of the business model. One may test a wine menu in a restaurant and realize that sales are not as large as the ones that same menu has in another similar restaurant in another town.

This may be due to many factors, and it's important to decide whether to pivot the menu or not. In AI, this pivoting is also important, and the software development strategy needs to be such that it can allow it. Reasons to pivot may include a new source of data that increases accuracy or lowers computational costs of the machine learning algorithms or that it is sound that users don't like the tone of the voice responses generated.

This case may be similar to the wine menu above, or perhaps there is a new channel to offer our services, and AI needs to be readapted or we're using a package like TensorFlow version two, and then all of a sudden code moves to a new version or to PyTorch, and we need to revisit all of our code, or many other reasons. Most importantly, flexibility needs to be built into the software development process because, as we said, when talking about stage one, the frontier of AI is rapidly moving, and it is important to incorporate adaptability into the design process. The reason may be mechanical.

Research on robotics at MIT is continuously exploring with new materials. And we are far from achieving human level performance. We don't even have a robot that can insert the key into a keyhole as well as humans can. By way of comparison, humans are born with 300 bones, ending up with 200 when adults. You also have muscles, tendons, ligaments, bursae.

In contrast, robots have at most a few hundred parts. As we build more and more complex mechanical robots, the associated software tinkering will be more sophisticated. This course is not about software development, but it is critical that you incorporate in your AI design process a basic software development plan. If you don't know how to do it, you can reach out to your technical team and make sure they explain you the basics. The more things we can automate at the development process, the better.

Here I'll name four things that are the minimum you'll have in place before starting. First, a code and data repository methodology. This includes establishing where the different versions of the code will be kept, and what tools to do so will be used. GitHub is one popular possibility that we use at MIT. You will probably need at a minimum a process to transfer code from development to testing to production. Part of the code repository must include documentation so that the code can be reused and executed.

Second, a testing and experimental plan. This means, how are you going to test the software? And how will you manage the different issues that arise from the testing plan? In particular, what are the methods you're going to track, and how are you going to make sure critical issues are addressed? Testing does not mean only software. It may also mean all of the things like business profitability, user acceptance, or even integration with the overall company product strategy.

Third, a GPU experimental set up that rationalizes the use of resources. GPUs or graphic processing units are the computers that do most of the number crunching for machine learning applications. The experimental setup should be such that the use of the available machines is maximized and optimized. If one uses a cloud supplier, it should be in the context of an optimized approach, computationally and financially.

And this brings us to the fourth and last. A plan with a budget to justify the investment. You should know that the rule of thumb is that new software development projects will cost two and a half times more than what you think they'll cost even after applying these rules. They always run over.

## Video 10: The Fourth Stage of the AI Design Process (Part 2)—AI Cancers

Last but definitely not least, the eighth decision, the second of this fourth stage, but the eighth overall in your design process is related to AI cancers and limitations. AI has some known issues that you'll have to plan ahead for. These are things we don't really yet know how to solve very, very well.

Here, I will talk about three of these cancers and how you may deal with them. The first one are adversarial attacks. Research has shown that you can fool any deep learning AI algorithm with simple modifications in the input signal. In the screen, you see an original image of a benign melanocytic mole that when combined with very low intensity adversarial noise, pulls the algorithm. One can prove theoretically that with deep learning, this is always possible.

Here is another example where sticker fools an algorithm into thinking that the banana is a toaster. More concerning is that researchers have been able to show that self-driving cars can be made to believe that a stop sign is a speed symbol sign, as you can see on the image. The image on the left does not fool the self-driving car, but the image on the right, does.

For the human eye, both cases are clear cases of stop signs, but it's just these little stickers that fool the system. And adversarial attacks can really compromise the security and privacy of the user. Research has recently been able to demonstrate that you can activate and control Siri with commands inaudible for the human ear, and you can make the phone do certain things.

The second cancer is lack of generalization. In many cases, AI cannot generalize properly. This happens, for example, in natural language processing as we sort of indicated earlier. Translation accuracy when going from language A to language B does not help when going from A to C. However, A to B and A to C does help B to C to a certain extent. In general, whether a machine learning algorithm will generalize or not is very hard to predict.

For example, face recognition algorithms run by Microsoft Azure or by Amazon Web Services have tens of millions of faces. Yet, they underperform with certain face colors and makeups because they have not been trained properly on this. Here, the issue is one of balancing datasets which makes generalization very difficult. If you overtrain on this forgotten skin colors and makeup styles, you may then skew the algorithms in another direction. A similar cancer is the one we cover next.

Onto the third cancer, bias. Machine learning algorithms often have the bias of the data that one uses to train them. For example, GPT-2, the precursor to GPT-3, had some fairly worrying biases, as you can see on the screen. The autocompletion was pretty biased because it reflected, you know, a lot of the literature that was input into the system that was old literature when text had very strong biases.

Similarly, Amazon had to scrap a recruiting tool had to scrap a recruiting tool because it showed male bias when recruiting engineering talent. This happened probably. We don't really know why, but it happened probably because males represent over 75% of the engineering workforce in most of the FAANGs. In fact, in all the ones that report the number.

Another related cancer is explainability. One of the big issues with modern deep learning algorithms is that they don't necessarily provide any insight into how they reach a conclusion. For example, you try to train an algorithm to distinguish wolves from dogs, as on the screen. And all the images from wolves have snow, like the one on the screen and none of the ones with dogs have snow. Perhaps because they are urban indoor pictures. It may be unclear how the algorithm is reaching the conclusion that a picture has a wolf or a dog. Perhaps it's simply distinguishing the scene backgrounds and not the foregrounds. Maybe it's easier to find whether there's snow or not. And there is a clear correlation in this example between the two discriminating tasks, wolves versus dogs or snow versus urban scene. But no real causality. In general, your AI algorithm needs to explain how it reach a conclusion. Perhaps deep learning is not your best choice.

The final cancer we'll discuss is unintended behavior. In one case, a robot in a shopping mall fell down the electric stairs and injured some customers. In another natural language example, a GPT-3 chat box installed inside the robot also in a retail environment, when asked by a person if suicide was a good idea, it answered, "Yes, I think you should do it." As another unintended behavior example, third one, the first vital self-driver car accident involved an urban Uber driver that was not paying attention, which, in fact, is probably what people will want to do in these vehicles. Uber probably would have to have had two drivers in the vehicle because of the extra effort to be attentive and not doing anything for very long periods of time.

Think about it. Think it's a lot harder to control a driver than to drive because you have to be most of the time doing nothing. But you have to be very alert. Therefore, your final list of decision needs to consider how you're going to minimize the impact of AI cancer. These five plus others that may emerge.

## Video 11: Conclusion

Okay. So, we are going to look now at an overview of the AI design process by looking at the four stages and the key decisions that have to be made. The first stage, stage one, is about intelligence. It's about deciding what is the intelligence that you want to incorporate in your AI algorithm.

Here there are two key decisions. One key decision is understanding the metrics. How are you going to measure that intelligence that you are trying to achieve? So, it's metrics. And the second one has to do with the scope. What's the scope of the intelligence that you want to apply? Give some insight into where that intelligence has to excel and where it's not that important. So, stage one. Now, when we move to stage one, we already have an intelligence, but where in the business are we going to use it?

Stage two is about really the business activity. And here again there are two key decisions related to AI. What is like the strategic role of AI? So, there's here a strategy role. And then the operational one. Here on strategy, there is a delta model that talks about three possible strategies, network externalities, best product, or full customer solution.

Then stage three is about the actual technology. You're making choices about technology. It's about AI tech. And here we talk about two important decisions that need to be made. One is the IP. What's the actual technical and scientific contribution you will be using, and you will be incorporating? Or maybe you develop your own, and you want to have your own patents or maybe you want to use third party fully available. So, that's one. And the second one is your data approach or your data strategy. And role models will be the FAANGs, you know, Facebook, Apple, Amazon, Netflix, Google.

And then finally the last stage is going to be stage four in your AI design process, and we call it tinkering. That's where you are going to put a lot of emphasis in your team, in your technical team, in actually implementing the software, testing it, and improving it. Two key decisions here will be your software development approach and how you're going to deal with AI limitations or what we call AI cancers.

But there are complementary assets here that will take most of your time so it's not just about AI if you're going to do successful implementation. And there's a bit of a full picture here with the eight decisions, four stages.