ALLIANZ GLOBAL CORPORATE & SPECIALTY

THE RISE OF ARTIFICIAL INTELLIGENCE: FUTURE OUTLOOK AND EMERGING RISKS

Allianz

About Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) is the Allianz Group's dedicated carrier for corporate and specialty insurance business. AGCS provides insurance and risk consultancy across the whole spectrum of specialty, alternative risk transfer and corporate business:
Marine,
Aviation (incl. Space),
Energy,
Engineering,
Entertainment,
Financial Lines (incl. D&O),
Liability,
Mid-Corporate,
Property insurance (incl. International Insurance Programs).

Worldwide, AGCS operates with its own teams in 34 countries and through the Allianz Group network and partners in over 210 countries and territories, employing almost 4,700 people of 70 nationalities. AGCS provides insurance solutions to more than three quarters of the Fortune Global 500 companies, writing a total of €7.4 billion gross premium worldwide in 2017.

AGCS SE is rated AA by Standard & Poor's and A+ by A.M. Best.

For more information please visit www.agcs.allianz.com or follow us on Twitter @AGCS_Insurance LinkedIn and Google+.

Contents

6 Executive Summary

Artificial Intelligence (AI) will bring new benefits and risks and transform insurance

8 Introduction

What is AI?

11 AI impacts on society

AI comes with potential benefits and risks in many areas: economic, political, mobility, healthcare, defense and the environment

14 AI areas of concern

Five areas of concern are crucial for identifying emerging AI risks: software accessibility, safety, accountability, liability and ethics

18 Emerging risks impact

Dealing with business risks, labor disruption, regulatory non-compliance and liability changes

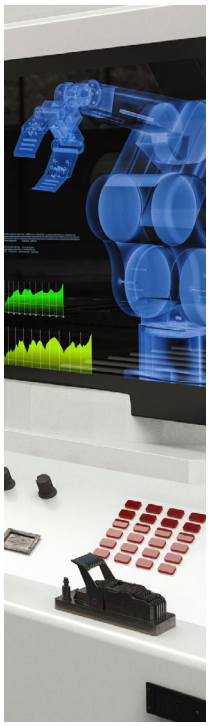
20 Case study: Autonomous vehicles

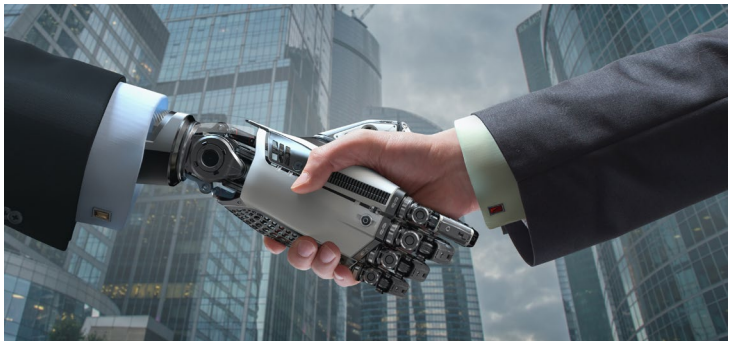
One of the most influential AI applications in future will bring benefits and complications

22 Impacts of AI on the insurance value chain

There are a number of ways in which AI could improve the insurance process

24 Contacts and credits





IN FOCUS

Artificial Intelligence (AI) refers to the ability of a computer program to think and learn like a human and its snowballing impact on society is undeniable. AI applications already pervade many industries, bringing potential benefits that have been predicted to double annual economic growth rate in a number of developed economies in future. However, the introduction of such innovative technology also brings new challenges. This paper identifies some of the emerging risk issues around the growing implementation of AI and examines possible future implications of so-called "strong" AI, outlining potential benefits and areas of concern. It also considers the transformative impact of AI on the insurance industry.

AI is predicted to boost labor productivity th
from analyzing data and automation of simp

rough new insights
ble tasks

Expectations for AI technology are rising and more development investments are being allocated in order to anticipate the benefits of more human-like or "strong" AI in future

EXECUTIVE SUMMARY

In addition to bringing a number of benefits, Artificial Intelligence (AI), like any disruptive technology, will also introduce new risks to society.

AI is projected to boost corporate profitability by an average of 38% by 2035[2]

From chatbots to autonomous cars, more widespread implementation of AI applications is transforming industry and society, bringing benefits such as increased efficiencies, new products and less repetitive tasks. AI technologies are projected to boost corporate profitability in 16 industries across 12 economies by an average of 38% by 2035[1].

Existing AI applications are built around so-called "weak" AI agents, which exhibit cognitive abilities in specific areas, such as driving a car, solving a puzzle or recommending products/actions. With the first tangible benefits of "weak" AI applications already being realized across many industries, expectations for AI technology are rising and more development investments are being allocated in order to anticipate the benefits of more human-like or "strong" AI in future. Its introduction will most likely be unprecedentedly disruptive to current business models.

Beyond being beneficial for several reasons, AI also comes with far-reaching implications for the **economy, politics, mobility, healthcare, security and the environment**. It will disrupt the labor market, changing the nature of long-established roles, and could be used to influence political thinking and opinion. Risks and benefits will appear in the short or long term depending on how long it takes for "strong" AI applications to be deployed in the real world. The rate of adoption depends on the level of investment in research and development in each application field.

For businesses, the potential threats could easily counterbalance the huge benefits of such a revolutionary technology. According to the **Allianz Risk Barometer 2018**, impact of AI and other forms of new technology already rank as the seventh top business risk, ahead of political risk and climate change[3]. Companies face new liability scenarios and challenges as responsibility shifts from human to machine. Meanwhile, increasing interconnectivity means vulnerability of automated, autonomous or self-learning machines to failure or malicious cyber acts will only increase, as will the potential for larger-scale disruptions and losses, particularly if critical infrastructure is involved.

AI is expected to improve safety in the mobility sector. It is estimated it could help reduce the number of road accidents by as much as 90%, but also brings questions about liability and ethics in the event of an incident occurring. Use of AI in the healthcare sector could eradicate many incurable diseases and help deliver care

[1,2] Accenture, How AI boosts industry profits and innovation, June 21, 2017
[3] Allianz Risk Barometer 2018. Based on 1,911 risk expert respondents

to remote areas but could also impact data privacy and patients' rights.

In the area of security and defense, AI-powered software will dramatically alter the digital security threat landscape. It could help to reduce cyber risk by better detecting attacks, but also increase it if malicious hackers are able to take control. AI could enable more serious incidents to occur by lowering the cost of devising cyber-attacks and enabling more targeted incidents. The same programming error or hacker attack could be replicated on numerous machines. Or one machine could repeat the same erroneous activity several times, leading to an unforeseen accumulation of losses. It is already estimated that a major global cyber-attack has the potential to trigger losses in excess of $50bn[1] but even a half-day outage at a cloud service provider has the potential for losses of $850m[2]. In addition AI could also enable autonomous vehicles, such as drones, to be utilized as weapons. Such threats are often underestimated.

On the subject of the environment, AI is already helping to combat the impact of climate change with smart technology and sensors reducing emissions. However, it is also a key component in the development of nanobots, which could have dangerous environmental impacts by invisibly modifying substances at nanoscale.

Appropriate risk management strategies will be needed to maximize the net benefits of a full introduction of AI into society. In order to manage long-term risks associated with adoption of advanced AI applications, five areas of concern need to be addressed: **software accessibility, safety, accountability, liability** and **ethics**. By addressing each of these areas, responsible development and introduction of AI becomes less hazardous for society.

In parallel, insurance will help to transfer and manage emerging risks. Traditional coverages – such as liability, casualty, health and life insurance – will need to be adapted to protect consumers and businesses alike. Insurance will need to better address certain exposures to businesses such as a cyber-attack, business interruption, product recall and reputational damage resulting from a negative incident. In addition, disruption to social norms will drive the need for solutions like **"universal basic income"** and other income protection schemes, likely backstopped by the evolution of current income protection insurance solutions.

AI could help reduce cyber risk but also increase it

AI raises concerns around personal data, particularly the extent to which this can be used to increase intelligence of agents. Data protection regulation in Europe already contains conspicuous limitations to adoption of AI systems. Businesses will need to reduce, hedge or financially cover themselves from the risks of non-compliance with new data protection regulations in future.

Meanwhile,assignment and coverage of liability will become more challenging in future. The application of new liability insurance models will likely be adopted – in areas such as autonomous driving, for example – increasing the pressure on manufacturers and software vendors and decreasing the strict liability of consumers.

However, AI will bring benefits to insurers as well as new risks. AI applications will improve the insurance transaction process, with many benefits already apparent. Customer needs can be better identified. Policies can be issued, and claims processed, faster and more cheaply. Large corporate risks, such as business interruptions, cyber security threats or macro-economic crises, can be better predicted. Chatbots can assist customers on a 24/7 basis.

Finally, insights gained from data and AI-powered analytics could expand the boundaries of insurability, extending existing products, as well as giving rise to new risk transfer solutions in areas such as non-damage business interruption and reputational damage.

[1] Lloyd's, Extreme cyber-attack could cost as much as Superstorm Sandy, July 17, 2017

[2] Allianz Risk Barometer 2018. Outage scenario is based on 50,000 companies in three specific industry sectors (financial, healthcare and retail) being impacted for 12 hours

INTRODUCTION

WHAT IS AI?

AI is a software that exhibits analytical, decision-making and learning abilities similar to those of humans. It is also a field in computer science that studies intelligent entities, not only from an engineering perspective, but also from a philosophical and psychological perspective[1]. Such a philosophical view is relevant especially when looking at the risks of a society where artificial and human intelligence co-exist.

From 1956, when the term **"Artificial Intelligence"** was coined, it took almost 25 years for the first commercial application to see the light with an intelligent agent that helped configure orders for new computer systems at Digital Equipment Corporation[2]. Today, AI spans applications in almost every industry and has been predicted to increase corporate profitability in 16 industries across 12 economies by an average of 38% by 2035[3]. AI improves productivity by substituting human tasks that can be constantly performed at no cost. For example, chatbots allow for around-the-clock virtual assistance. Additionally, AI enables tasks that require specialist expertise, such as specialized medical diagnoses.

AI is capable of substituting for humans essentially because of five characteristics which are progressively more sophisticated (*see box*).

HOW AI CAN SUBSTITUTE FOR HUMANS

1. Processing of large amounts of data, with higher speed and capacity than humans
2. Learning from example data
3. Recognizing objects and their association to a situation
4. Inferring the future state of an object or situation
5. Identifying an optimal decision based on past, present and inferred future states

[1,2] Russell, S. and Norvig, P. , Artificial intelligence: A modern approach, Prentice-Hall, 1995
[3] Accenture, How AI boosts industry profits and innovation, June 21, 2017

FROM "WEAK" TO "STRONG" AI

One of the most advanced AI applications is autonomous driving. Despite the cleverness of the autonomous pilot in making complex driving decisions, differently from a human, the same "artificial brain" would not be able to complete other tasks, such as picking stocks or playing chess, without an increase in computing power.

AI "smartness" is proportional to the amount of learned data and not based on high-level semantic concepts such as "risk", "competition", "pay-back", "goal", "fairness", etc. Humans, instead, can learn new concepts without expanding their brain or necessarily seeing examples. They can learn new concepts by associating them to higher-level representations and exploiting the creative process. Such a difference between how AI and humans learn and conceptualize the world is what differentiates current from future AI systems, respectively "**weak" AI** and "**strong" AI**.

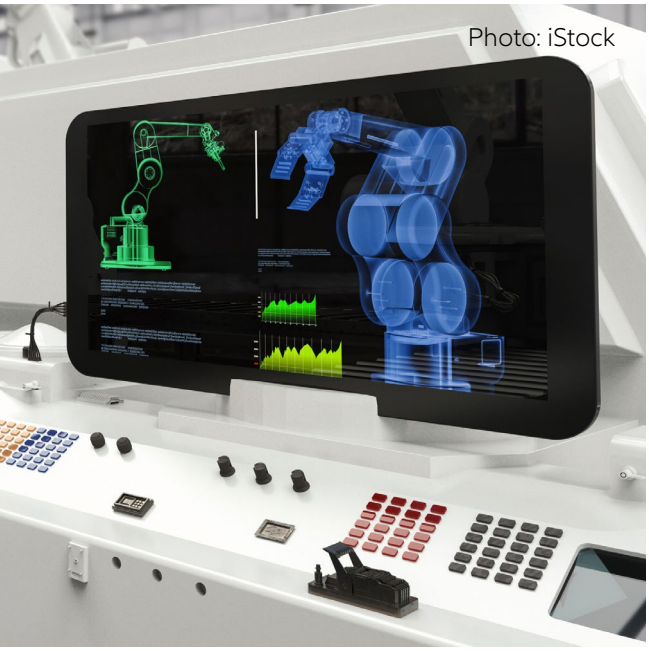


Photo: iStock

AI is already increasingly evident in industries such as smart manufacturing

"WEAK" VS. **"STRONG"** AI

"Weak" or **"narrow" AI** refers to the AI being deployed in business today – e.g. chatbots. In contrast, **"strong" AI**, a machine with consciousness, sentience and mind – or artificial general intelligence that approaches human cognitive abilities – are theoretical and not yet deployed in business.

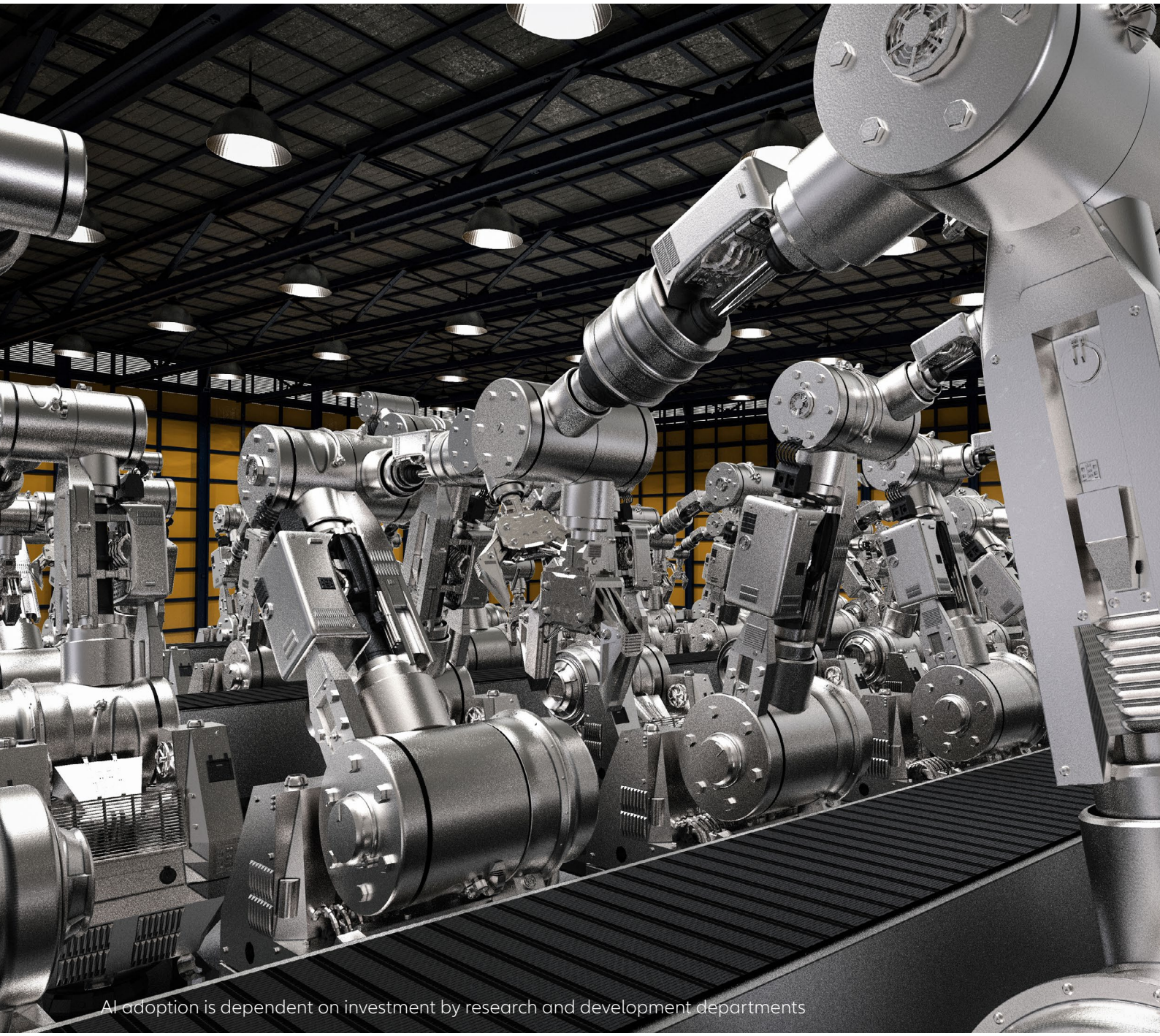
All existing AI applications are built around "weak" AI agents, which exhibit human-like cognitive abilities in specific areas of competence, such as driving a car, solving a puzzle, recommending products or actions, or making a medical diagnosis. Such "weak" AI agents can solve problems in complex yet delimited domains. Concrete examples of "weak" AI agents in the insurance industry are customer service chatbots. Allianz, for example, has developed **Allie**[1], an online assistant available 24/7 to answer customers' questions. It has also developed a claims chatbot in Singapore.

On the other hand, "strong" AI agents exhibit human-like intelligence and the intrinsic ability to generalize and create new concepts. "Strong" AI agents are not necessarily as conscious as humans in experiencing the self and the surrounding context, but they have the ability to generalize concepts and solve problems never seen before, pretty much like humans. "Strong" AI agents are expected on the market around 2040[2]. They are a hypothetical machine that exhibits behavior at least as skillfully and as flexibly as humans do. At present, "strong" AI agents do not exist.

Although current attention around AI is focused on existing "weak" AI applications, a more forward looking approach on AI risks considers "strong" AI agents, because their introduction will most likely disrupt society as we know it.

"Strong" AI agents are expected on the market around 2040

[1] http://allie.it
[2] Müller, V. and Bostrom, N. Future progress in artificial intelligence: A survey of expert opinion, Fundamental Issues of Artificial Intelligence, 2016



AI adoption is dependent on investment by research and development departments

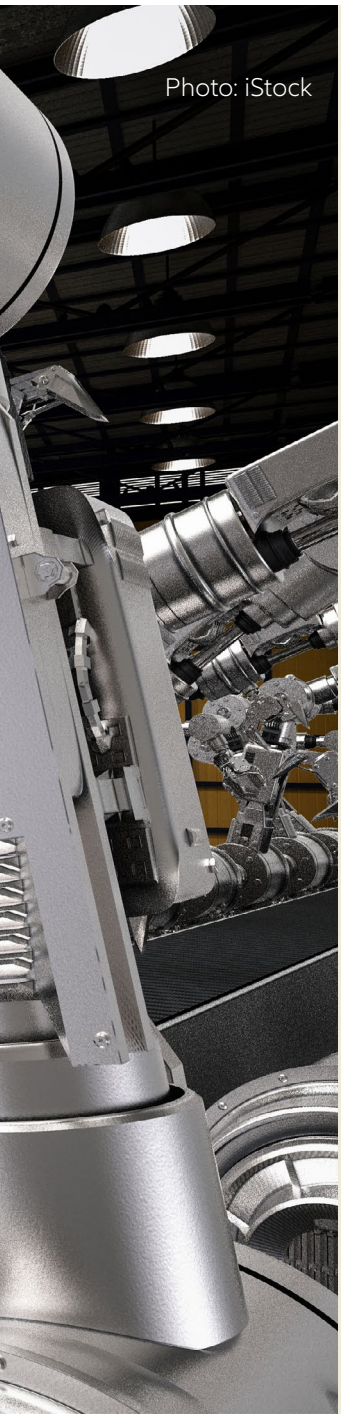


Photo: iStock

AI IMPACTS ON SOCIETY

The disruptive impact of “strong” AI applications affects all of society. Given its broad scope of application, AI comes with potential benefits and risks in many areas: economic, political, mobility, healthcare, defense and environmental. Risks and benefits can appear in the short- or long-term depending on how long it takes for “strong” AI applications to be deployed in the real world. The rate of adoption depends on the level of investment in research and development in each application field.

ECONOMIC IMPACTS

While AI is predicted to bring increased GDP per capita[1] by performing existing jobs more efficiently and compensating for a decline in the workforce, especially due to population aging, the potential substitution of many low- and middle-income jobs could bring extensive unemployment. For example, construction firm Mace predicts 600,000 of the current 2.2 million jobs in the industry could be automated by 2040[2]. Such scenarios will require new ways of determining liabilities and mitigating risks of social security. For example, universal basic income[3] or robot taxation[4] could be introduced by governments to enable everyone to benefit from the automation and "**robotization**" of society. Ethical considerations on the meaning of work[5] and the collaboration between human and artificial intelligence[6] in the workplace will also be relevant to shape policymaking and corporate strategies.

Wider ethical concerns cover the degree by which machines should substitute humans in critical activities such as surgery, medical treatment, law-making and governmental decision-making. If machines prove to be better than humans, there may be fewer human practitioners and society may lack human knowledge on performing such critical activities.

POLITICAL IMPACTS

Adoption of AI and analytics technologies allow for the screening of an individual's political agenda and checking of candidates' credibility. If controlled by only a few major players it may generate the opposite effect, facilitating governmental influence through individualized

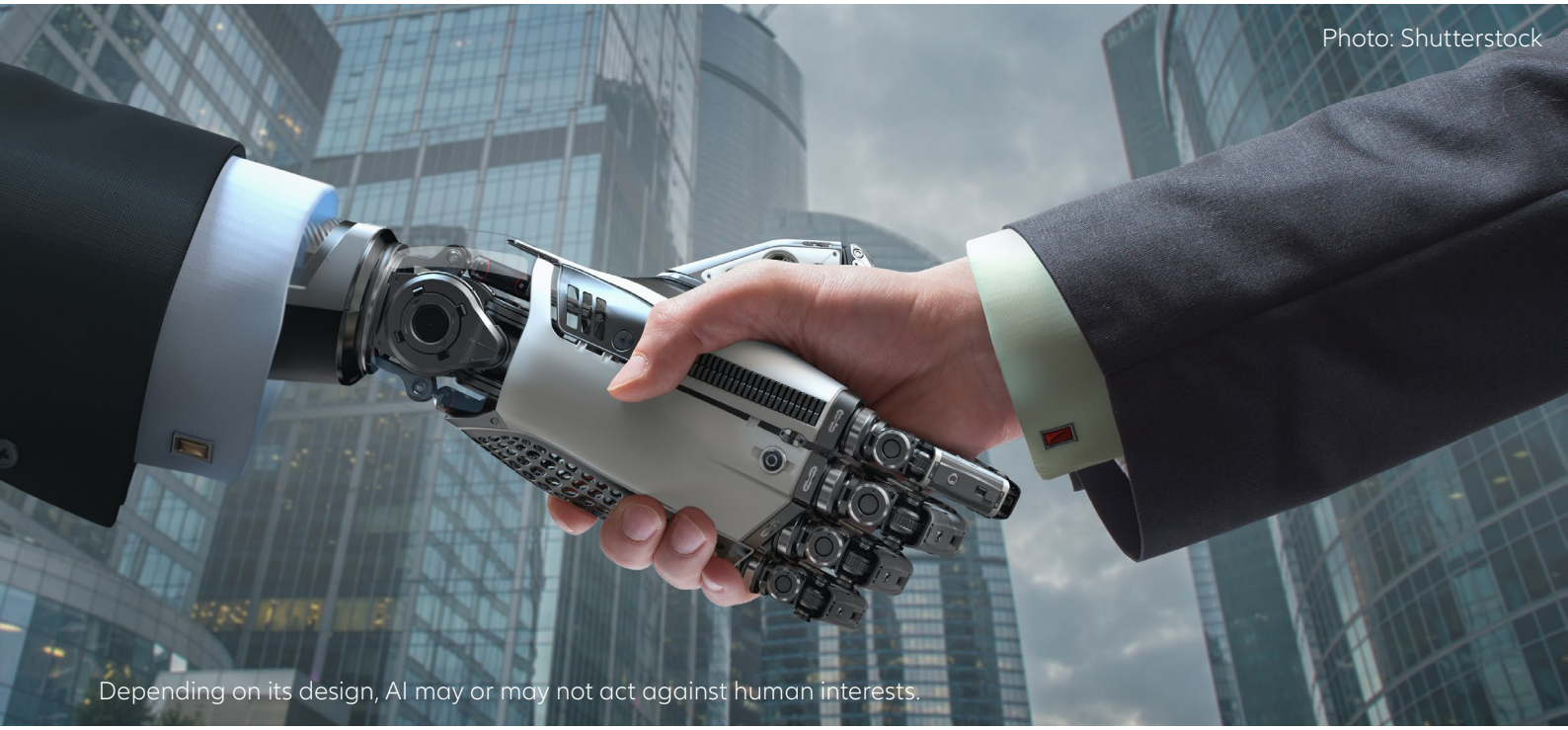


Photo: Shutterstock

Depending on its design, AI may or may not act against human interests.

[1] PricewaterhouseCoopers (PwC), AI Analysis, Sizing the Prize, 2017
[2] The Telegraph, Rise of the robot brickie: Automation could wipe out 600,000 construction jobs by 2040, October 30, 2017
[3] Intereconomics, The basics of basic income, 2017
[4] Handelsblatt Global, A tax on robots?, February 28, 2017
[5] Pink, Daniel. Drive: The Surprising Truth About What Motivates Us. 2009
[6] McKinsey Quarterly, Where machines could replace humans - and where they can't (yet). July 2016

steering of citizens' preferences. AI-powered chatbots tailor their communication approach to influence individual users' decisions. In the UK, a form of initial computational propaganda has already happened during the Brexit referendum[1]. In future, there are concerns that oppressive governments could use AI to shape citizens' opinions.

MOBILITY IMPACTS

AI is expected to improve mobility. AI-powered self-driving cars are predicted to eliminate human errors, which are the main cause of accidents. Transport management systems will manage transport demand depending on available infrastructure capacity and connectivity. Despite the promise of streamlined travel, AI also brings concerns about who is liable in case of accidents and which ethical principles autonomous transportation agents should follow when making decisions with a potentially dangerous impact to humans, for example, in case of an accident.

HEALTHCARE IMPACTS

Healthcare is the sector where AI is probably expected to deliver the most societal benefit. For example, by using advanced data analytics, sequencing of human DNA will allow the eradication of many incurable diseases, including cancer. Enhanced cognitive abilities will allow AI agents to give specialist medical advice and to diagnose diseases that otherwise would require identification and cross-validation of a high number of medical observations.

Quality of life and life expectancy is expected to increase. In addition, scarce availability of medical expertise in remote areas of the planet will be managed through AI-based mobile medical advice.

However, the use of advanced AI for elderly- and child-care are subject to risk of psychological manipulation and misjudgment *(see page 17)*. In addition, concerns about patients' privacy when AI uses medical records to research new diseases is bringing lots of attention towards the need to better govern data privacy and patients' rights.

SECURITY AND DEFENSE IMPACTS

AI-powered software has a huge potential to boost global security as well as reduce business risks by helping to detect cyber-attacks[2] and identify terrorist activities. Monitoring and analyzing social media, financial transactions and other large datasets already supports security intelligence in identifying and predicting threats before they happen. AI can support developing complex and reliable "what-if" scenarios in order to evaluate potential long-term outcomes. Conversely, misuse of strong AI may also increase risk of cyber-attacks if malicious hackers train AI to attack. Autonomous weapons, such as drones, could also be utilized[3]. Such threats are often underestimated.

ENVIRONMENTAL IMPACTS

AI could help fight one of the toughest challenges of this century – climate change. By leveraging AI technologies, smart cities and smart grids are already reducing emissions per capita. In addition, AI-powered robots can be deployed in harsh environments exposed to toxic or harmful materials. On the other hand, AI is a key component for the development of nanobots, which could have dangerous environmental implications by invisibly modifying substances at nanoscale. For example, nanobots could start chemical reactions that would create invisible nanoparticles that are toxic and potentially lethal[4].

Healthcare is the sector where AI is probably expected to deliver the most societal benefit

[1] Howard, P. N. and Kollanyi, B. Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum, June 21, 2016
[2] Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, System predicts 85 percent of cyber-attacks using input from human experts, April 18, 2016
[3] Future of Life Institute, Autonomous weapons: An open letter from AI and robotics researchers, July 28, 2015
[4] Bass, Carole. "Nanotech, The Unknown Risks", Yale Education, 2008

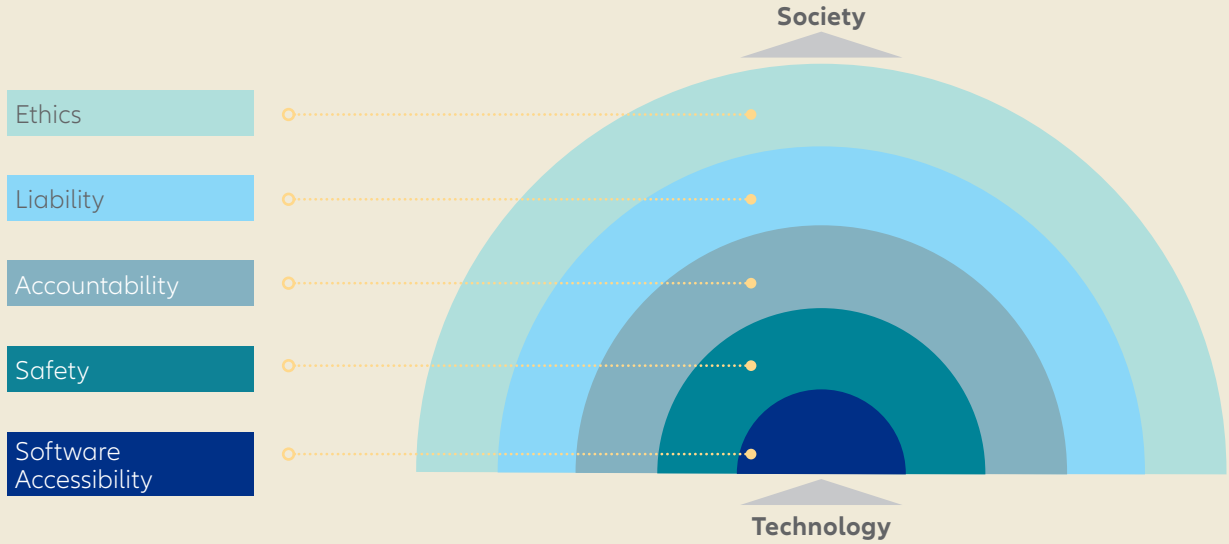
AI AREAS OF CONCERN

The path towards "strong" AI is paved with as many concerns as opportunities. Current AI systems are capable of making decisions, boosting operational efficiency and generating new products. The unprecedented acceleration of applications where AI can solve complex problems better than highly-skilled human specialists, e.g. detecting skin cancer[1], is counterbalanced by the inability of AI developers to predict negative impacts of some applications.

For example, the Microsoft Tay AI experiment, in which an AI bot named Tay was kicked off of Twitter the same day it launched "for becoming a sexist, racist monster", showed how a chatbot could be deceived to learn bad human behaviors[2]. Meanwhile, Facebook recently shut down an experiment when two chatbots developed their own language to talk to each other[3]. This two-sided reality elucidates the importance of careful scrutiny of the impacts of advanced AI technology before it is rolled out to society and uncovers the foundational problem of developing "strong" AI applications capable of making high-quality decisions. The problem is defined by Stuart Russell, AI pioneer and expert, as "the value alignment problem" which consists of aligning AI values and goals with those of humans[4].

Five areas of concern are crucial for identifying emerging AI risks, namely **software accessibility, safety, accountability, liability and ethics.** By addressing each of these areas, responsible development and introduction of AI becomes less hazardous for society.

FIVE AREAS OF CONCERN ABOUT "STRONG" AI*



Source: Allianz Global Corporate & Specialty

** Size of circle represents estimate of the amplitude of the impact on society*

[1] Stanford News, Deep learning algorithm does as well as dermatologists in identifying skin cancer, January 25, 2017
[2] TechRepublic, Why Microsoft's 'Tay' AI bot went wrong, March 24, 2016
[3] The Daily Mail, Facebook shuts down controversial chatbot experiment after AIs develop their own language to talk to each other, July 31, 2017
[4] Russell, Stuart. Of Myths and Moonshine, 2017

SOFTWARE ACCESSIBILITY

Software accessibility concerns whether AI code should be closed or open to the public and in particular to the software development community.

AI's key component is software, which is accessible to almost anyone since it does not generally require huge monetary funding . Therefore, AI applications can be potentially developed by anyone who has access to open software code repositories, which allow users to host and review code, manage projects and build software alongside other developers. This increases the risk of unintended, and potentially catastrophic, consequences due to technology misuse. Risks are higher in areas such as cyber security, defense and medical applications.

Overall, there are both pros and cons to ensuring open accessibility to AI code[1]. On one hand, open sourcing potentially accelerates development of AI and allows society to equally benefit from the advantages of "strong" AI. Openness decreases the probability that only a small group of first-moving companies or research centers can have control of AI and unintentionally generate negative impacts. It also enables industry outsiders, such as insurers, to control such impacts through risk analysis, auditing and safety engineering.

On the other hand, closing access to software may prevent appropriation and misuse of "strong" AI from developers with harmful intentions. However, without open sourcing, the time to achieve "strong" AI status and reap its benefits may be longer and if the first-movers turn out to develop a harmful AI, it would be difficult for the rest of the community to keep up with the maturity of technology and develop preventive counter-activity measures.

SAFETY

Preventive measures that reduce risk from unintended consequences are essential[2]. AI safety is concerned with ensuring that an AI system is tested in an environment similar to the real world so that its goals and behaviors are appropriately specified and the system can be safely introduced into society. A misalignment between the developer's objective and the interpreted goal of the AI agent can cause unexpected accidents that are apparent only when the system is introduced into the real world.

The race for bringing AI systems to the market incentivizes developers to underestimate crucial software verification and validation activities guaranteeing deployment of safe AI agents. For example, a poorly designed AI agent for portfolio management, with the objective of maximizing profits by investing in assets within a certain category of investment risk, may work according to specifications when tested in a development environment where the agent can pick from a few assets predefined by the developers. When introduced into the real world, however, the agent may behave unexpectedly when it discovers that return on investments could be maximized by first investing the available capital resources into non-legal activities.

As the number of systems connected to the internet increases, cyber security will have an increasingly high economic impact on society, nowadays estimated in the tens of billions of dollars, so the introduction of increasingly more advanced AI systems to which society will be dependent amplifies the negative impact of unsafe ones. AI safety, however, has lately gained recognition and momentum, especially in the academic community, showing a compounded annual growth of investments roughly equal to 75%[4].

A cyber-attack impacting a cloud provider could trigger $50bn+ of economic losses[3]

Cyber security will have an increasing economic impact on society

[1] Global Policy Journal, Strategic implications of openness in AI development, February 9, 2017
[2] arXiv preprint, Concrete problems in AI safety, June 21, 2016
[3] Lloyd's of London Press Release, Extreme cyber-attack could cost as much as Superstorm Sandy, July 17, 2017
[4] Centre for Effective Altruism, Changes in funding in the AI safety field, February 1, 2017

The area of AI safety has shown compounded annual growth of investments roughly equal to 75%[4]

ACCOUNTABILITY

Beyond responsible software development and testing, accountability refers to the ability of an agent to make transparent and auditable decisions. With the proliferation of AI agents programmed to make decisions, regulators face the increasingly significant question of how to ensure that not only data input but also the process leading to AI-made decisions can be reviewed and audited, for example, by appropriate oversight bodies including lawyers, AI experts and final users[1].

The basis for accountability of an AI agent is transparency of its decisions, regarded as the interpretability and reproducibility of the decision-making process so that a human can explain it with logical reasoning. Consumer protection regulation addresses transparency as the **"right to explanation"**[2], In other words, everyone should be given the right to know what brought the agent to a conclusion and be able to query it on possible different decisions.

The importance of accountability in precluding unintended consequences from AI applications is also due to the fact that input data used to train AI algorithms is usually human-generated. As such, training data contains prejudice and implicit bias. Therefore, AI agents tend to amplify the effect of such prejudices and biases[3], resulting in partial and unfair decisions.

For example, autonomous chatbots trained on language texts are prone to learn and perpetuate human prejudices and unfairness. Transparency of the decision-making process and the underlying training data would ensure that the outcome is unbiased and impartial regardless of a consumer's characteristics such as race, gender or religion. Such transparency can be enabled by setting up appropriate scrutiny requirements for the AI development process.

LIABILITY

While AI agents could take over many decisions from humans they cannot legally be liable for those decisions. Generally speaking, the manufacturer of a product is liable for defects that cause damages to users. The same applies to a producer of AI agents in case of damages due to defects in design or manufacturing. However, AI decisions that are not directly related to design or manufacturing, but are taken by an AI agent because of its interpretation of reality, would have no explicit liable parties, according to current law. Leaving the decision to courts may be expensive and inefficient if the number of AI-generated damages start increasing[5].

The general difficulty in establishing a clear liability and regulatory framework around AI is mainly due to the complications of identifying impacts of AI technologies before products get to the market and can be tested in the real world. Even when products are in the market, it becomes difficult to identify what can exactly go wrong before damages take place.

A solution to the lack of legal liability would be to establish an experts-based agency with the purpose of ensuring AI safety and alignment with human interests. The agency would have certification powers and would establish a liability system under which designers, manufacturers and sellers of AI-based products would be subject to limited tort liability, while uncertified programs that are offered for commercial sale or use would be subject to strict joint and several liability[6].

ETHICS

Ethical concerns are more and more important once AI pervade society.

Decisions taken by AI agents are in many cases faster, more accurate and more suitable to complex and dynamic contexts than decisions taken by humans. However, in some situations there is no objective view on what the optimal decision should be, because the optimal decision is subjective and depends on the ethical principles adopted to draw conclusions.

[1] University of Pennsylvania Law Review, Accountable Algorithms, 2016
[2] Goodman, Bryce, and Flaxman, Seth. EU regulations on algorithmic decision-making and a "right to explanation". International Conference of Machine Learning workshop on human interpretability in machine learning,2016
[3] Science, Semantics derived automatically from language corpora contain human-like biases. April 14, 2017
[4] Centre for Effective Altruism
[5] The Law Society of England and Wales, Written evidence submitted by the Law Society (ROB0037), April 2016
[6] Harvard Journal of Law & Technology, Regulating artificial intelligence systems: Risks, challenges, competences and strategies, Number 2, 2016

Neither developers, nor the law, can establish such objective rules. AI agents need to decide based on their interpretation of the situational context, of the stakeholders and the stakes involved.

Such an interpretative effort is complicated for AI agents, which are unable to comprehend abstract concepts such as loyalty, happiness, hurt or values. The consequence is that depending on its design or the information upon which it is trained, an AI agent may act against human interests.

Consider the following example, from the field of elderly care: An AI robotic agent is trained to maximize the well-being of an elderly woman with deteriorating health due to Parkinson's disease. The agent provides her with continuous care and attention in avoiding risky situations that can injure her. But in order to reduce the risk of falls, the AI agent starts controlling her opportunities to get out of her apartment. While this approach effectively reduces risk of injury and does not deteriorate her physical condition, it reduces her social contact, leading to a spiral of depression. This example shows that an AI may not have "bad intentions" per-se, but its actions may have a negative impact if its range of goals are poorly designed. Such concerns are increasingly relevant for applications where users are sensitive, such as children, in addition to the elderly[1].

The challenge when developing AI agents is to instill the agent with a distinction between good and bad. One way is to let the agent observe human behavior in different situations and act accordingly. The longer humans are observed, the more virtuous, according to human standards, an AI agent becomes. However, humans have prejudices and biases.

IMPACTS OF "STRONG" AI BY AREA OF CONCERN*

	Impacts		Areas of Concern				
	Positive	Negative	Software Accessibility	Safety	Accountability	Liability	Ethics
Economic	• Increased productivity • Talent shortage compensation	• Increased income disparity • Markets monopolization				!	!
Political	• Reality checks and screening of political agendas	• Biased influence through citizen screening and tailored propaganda • Potential exploitation by totalitarian regimes	!		!		
Mobility	• Autonomous driving brings improvement in road safety	• Cyber security • Liability issues in case of accidents				!	!
Healthcare	• Reduction of diseases through advanced DNA sequencing • Personalized medical and health advice anywhere, anytime	• Alteration of social relationships may induce psychological distress • Social manipulation in elderly- and child-care			!		!
Security & Defense	• Increased cyber intelligence towards potential terrorist threats	• Catastrophic risk due to autonomous weapons programmed with dangerous targets	!	!			
Environment	• Energy consumption optimization • Accelerated invention of solutions to reduce global warming	• Accelerated development of nanotechnology produces uncontrolled production of toxic nanoparticles	!	!			

** Exclamation marks for each type of impact indicate the two most relevant areas of concern.*

Source: Allianz Consulting and Allianz Global Corporate & Specialty

[1] Ethics and Information Technology, Granny and the robots: Ethical issues in robot care for the elderly, March 2012

EMERGING RISKS IMPACT

The potential impact of AI on the insurance industry is twofold. Its application will help to improve the insurance process in a number of other ways *(see pages 22-23)*, benefiting the customer. In addition, it will have a more disruptive impact by introducing new risks. However, these could be transferred through the development of potential new insurance products (especially in the areas of liability, casualty, health and life) for protection of businesses and consumers.

BUSINESS RISKS

67% of CEOs think that AI will have a negative impact on stakeholder trust over the next five years[2]

According to a recent survey of global CEOs, 67% believe AI and automation will have a negative impact on stakeholder trust in their industry over the next five years[1].

AI exposes business to threats that could easily counterbalance the huge benefits of such a revolutionary technology. Businesses will face new liability scenarios from the possible shift of responsibility from human to machine *(see page 19)*. Meanwhile, increasing interconnectivity means vulnerability of automated, autonomous or self-learning machines to failure or malicious cyber acts will only increase, as will the potential for larger-scale disruption events, and subsequent losses, particularly if critical infrastructure, such as IT networks or power supply, are involved.

The same programming error or hacker attack could be replicated on numerous machines. Or one machine could repeat the same erroneous activity several times, leading to an unforeseen accumulation of losses and difficulties in identifying what went wrong. It is already estimated that a major global cyber-attack has the potential to trigger losses in excess of $50bn[3]. However, even a half-day outage at a cloud service provider could result in losses of $850m[4]. This latter scenario is based on 50,000 companies in the financial, healthcare and retail sectors being impacted for 12 hours.

While AI can be used to detect and prevent cyber-attacks, the opposite is also possible. AI could facilitate more serious incidents by lowering the cost of devising new tools and weapons to launch attacks. It could also be used to develop more targeted attacks. AI could even be used in future to weaken cyber defense mechanisms by utilizing social engineering to psychologically manipulate people into performing actions or divulging confidential information.

Ultimately, whatever the cause, the slightest unintentional error caused by AI could quickly escalate into a major incident, damaging reputation and ultimately the bottom line.

LABOR DISRUPTION

One of the main societal consequences of AI will be disruption of job markets. On one side, AI will facilitate search and even substitution of missing talent. On the other side, in future many repetitive jobs such as postal clerks, or travel agents, may not exist anymore[5].

[1, 2] PricewaterhouseCoopers, 20th Global CEO Survey, 20 years inside the mind of a CEO...What's next?, 2017
[3] Lloyd's, Extreme cyber-attack could cost as much as Superstorm Sandy, July 17, 2017.
[4] Allianz Risk Barometer 2018 www.agcs.allianz.com/insights/expert-risk-articles/arb-2018-business-interruption/
[5] McKinsey Global Institute, Future that works: Automation, employment and productivity, January 2017

In order to protect citizens from loss of income, governments are experimenting with different forms of public subsidies where the increased tax income from AI- and automation-driven business productivity is redistributed among the unemployed or the whole population. For example, "**universal basic income**"[1], which has already been subject to a vote in Switzerland, is the most discussed subsidy scheme comprising a fixed amount of money redistributed to every citizen regardless of social status or income. In the absence or insufficiency of such government-supported formulas, evolution of current income protection insurance policies will most likely protect against particular unemployment circumstances related to job automation.

Automation and AI will bring more free time and consequently increase the likelihood of new businesses being started. New types of investment coverage to financially support entrepreneurs against the risks of starting new ventures will likely be introduced. For example, **Allianz X** is the digital investment unit of the Allianz Group, which invests in start-ups relevant to the insurance sector.

REGULATORY NON-COMPLIANCE

High-paced technological advances in AI will increase governmental challenges to protect consumers from the negative consequences of inappropriate uses of technology. Frequency of regulatory updates will increase.

Consumer protection regulation will require careful understanding of how AI-based sales agents impact consumers' decisions. With current AI agents acting as "black boxes" in giving recommendations without clearly explainable rationales, new regulations and governmental directives may emerge. The best risk management solution is likely to be control, by having human supervisors controlling and explaining AI agents decisions.

Data protection regulation will focus more on defining the extent to which data, especially personal data, can be used to increase intelligence of AI agents. In fact, data protection regulation in Europe[2] already contains conspicuous limitations to adoption of AI systems. In future, businesses will need to reduce, hedge or, at worst, financially cover themselves, from risks of non-compliance with new data protection regulations.

LIABILITY CHANGES

Assignment and coverage of liability will become more challenging in future due to the possible shift of responsibility from human to machine and, therefore, to the manufacturer or its suppliers. Liability may arise from a product defect. It could even result from communication errors between two machines or between machine and infrastructure. Recalls could even become larger and more complex. If a series of accidents raises concerns for the AI technology behind driverless cars, it could trigger a massive recall across different manufacturers and countries.

Autonomous driving is probably the most well-known upcoming AI application. Current automobile insurance policies are based on the principle that the car owner is responsible for both individual driving mistakes and defects of the vehicle due to maintenance.

With autonomous driving, the ratio of cases in which insurers will need to get compensation from car manufacturers and AI software providers will drastically increase, because the human user will be often out of the loop. Therefore, new liability models resembling product liability, where manufacturers take over liability for product defects, will probably be adopted. Compulsory motor insurance will then be extended to include product liability coverage, giving motorists cover when they have handed full control over to the vehicle. In this case, motorists or insurers will rely on courts to apply the existing rules of product liability under the common law, to determine who should be held responsible[3].

With autonomous driving, the ratio of cases in which insurers will need to get compensation from manufacturers and AI software providers will drastically increase

[1] Compass, Universal basic income: An idea whose time has come?, 2016
[2] Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), May 4, 2016
[3] Centre for Connected & Automated Vehicles (UK), Pathway to driverless cars: Proposals to support advanced driver assistance systems and automated vehicle technologies, 2016

CASE STUDY: AUTONOMOUS VEHICLES

Autonomous vehicles are expected to be the most influential AI application in future. The penetration rate for autonomous vehicles is expected to reach 5% by 2030, with a compounded annual sales growth rate of about 40% projected between 2025 and 2035[1]. Given the upcoming market disruption, the automotive and insurance industries are driving the identification of potential risks and opportunities.

BENEFITS

Autonomous vehicles will enhance road safety by removing human error, the main cause of road accidents. AI is predicted to drastically reduce the number of road accidents by 90% and CO2 emissions by 60%[2].

Monetary benefits in terms of crash savings, travel time reduction, fuel efficiency and parking benefits are estimated to be between $2,000 to $4,000 per year, per vehicle[3].

COMPLICATIONS

Autonomous vehicles use sophisticated combinations of sensors and AI software to make hundreds of decisions per minute in order to cope with dynamic traffic conditions. There are many constraints which complicate the decision-making process: fuel economy, level of comfort, compliance with regulation, driver safety and environment protection. AI agents can still cope with these complex decision points as long as they can follow clearly defined models and rules. If such models and rules were accurately defined and autonomous vehicles could literally interpret and follow them, there would be no space for unpredictability and no need for insurance.

But for certain decisions there are no established universal rules. For example, running over three pedestrians versus sacrificing its only passenger to save them is a decision that requires choosing between two negative scenarios. Although a human driver would usually save itself it would still take decisions on pedestrian's lives on the basis of individual ethical principles[4]. An AI driver would need to decide according to some principles. Differently than a human, an AI driver can be programmed by design to act according to principles which may save pedestrians and turn against the driver.

IMPLICATIONS

Most of the arguments in favor of AI are to make roads safer. However, risks may shift and may require new types of coverage to be engineered.

Personal risk and liability coverage will be needed to protect passengers from autonomous vehicles making decisions that, even if taken according to design, turn against the driver. Seemingly, new product liability coverages will be needed to protect manufacturers against undesired autonomous vehicles' decisions that damage either passengers, pedestrians or goods.

[1] IHS Markit, Autonomous vehicle sales forecast to reach 21 mil. globally in 2035 according to IHS Automotive, July 6, 2016
[2] McKinsey and Company, Ten ways autonomous driving could redefine the automotive world, June 2015
[3] Transportation Research Part A: Policy and practice, preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations, 2015
[4] Science, The social dilemma of autonomous vehicles, June 24, 2016

Most arguments in favor of driverless cars are about safer roads, but risks may shift, requiring new types of insurance coverages

IMPACTS OF AI ON THE INSURANCE VALUE CHAIN

AI will also influence how insurance provides value to customers. In other words, current AI applications improve the insurance value chain by making it more effective in appropriately targeting customer needs and efficient in delivering value on time and at lower cost.

The most common applications directly relevant for the insurance value chain are described below. Such applications improve the profitability of insurance by delivering more customer value at lower cost and more quickly.

INTELLIGENT AI-GENTS

In future, AI will support underwriters with analysis of data and assessment of risks. There are many areas – such as reputation, cyber, supply chain and economic and climate risk scenarios – where machine learning could help companies better understand their risks.

AI could also work alongside other new technologies, such as blockchain, to enable new, faster and more customized services. For example, sensors on shipping containers are already providing data on the location and condition of cargo, which, once analyzed, can trigger insurance cover or mitigation measures if the goods are damaged.

Insights gained from data and AI-powered analytics could expand the boundaries of insurability, extending existing products, as well as giving rise to new risk transfer solutions in areas such as non-damage business interruption and reputational damage.

HOW AI IS IMPACTING THE INSURANCE TRANSACTION

CUSTOMER/MARKET MANAGEMENT

- Individualized campaign generation
- Market analysis and forecasting

CUSTOMER ADVISORY

- Needs discovery
- Product recommendation

"Weak" AI applications with direct impact on the insurance value chain

CUSTOMER/MARKET MANAGEMENT

As opposed to other industries, the insurance sector is characterized by a relatively low frequency of customer interaction (often customers reach out to the insurer only when buying a product or submitting a claim). Therefore, the ability to utilize customer data to understand customer preferences is crucial.

AI can help by sorting through and analyzing customer information and providing accurate customer profiles to create successful individualized marketing campaigns.

Additionally, AI helps make sense of huge amounts of market data, including economic demand, competitors' offerings and market volatility, in order to price products according to current and forecasted demand.

CUSTOMER ADVISORY

AI applications also support the process of recommending new products to prospective customers. Specifically, by automatically matching individual customer profiles and goals to available offered products, the product recommendation process is faster and more effective. Given the inherent complexity of insurance products, AI can provide individualized product illustrations and help customers discover their insurance needs, especially with respect to complex products such as life savings.

POLICY PURCHASING

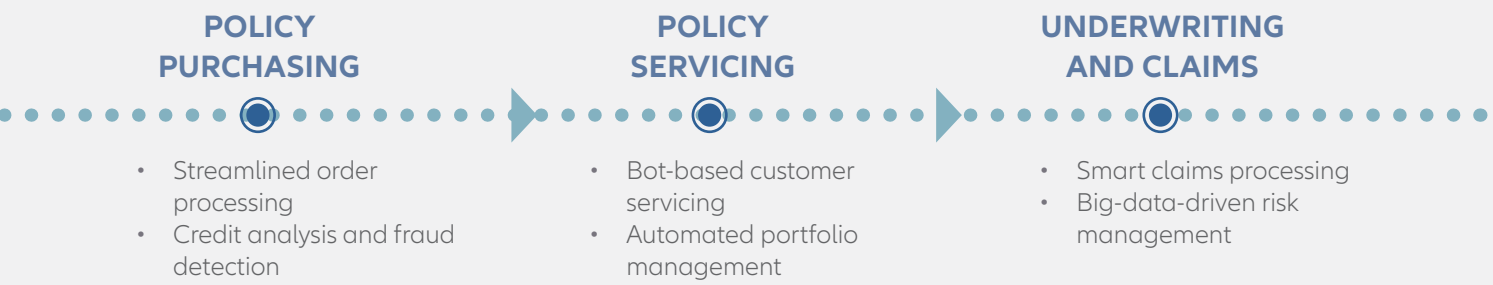
During purchasing, and before submission to underwriting, an insurance policy needs to be processed and screened. Such a process may take hours or even days if performed manually. AI allows for the automatic processing of orders by performing various types of data-checking and fact-checking, such as fraud detection and credit analysis. The result is increased customer experience through a faster purchasing process.

POLICY SERVICING

When an insurance policy is in-force, chatbots can assist customers on a 24/7 basis. Moreover, policy adjustments such as portfolio diversification and risk profiling can be automatically performed by AI-based algorithms.

UNDERWRITING AND CLAIMS

Given the large availability and timeliness of data available on economic, demographic, environmental, and market conditions there is a vast potential for more refined definition of risk. AI supports interpretation of risk data to provide actuaries with cutting edge models for efficient risk management.



CONTACT US

For more information contact your local Allianz Global Corporate & Specialty (AGCS) Communications team:

London
Michael Burns
michael.burns@allianz.com
+44 203 451 3549

Munich
Heidi Polke-Markmann
heidi.polke@allianz.com
+49 893 800 14303

New York
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

Paris
Florence Claret
florence.claret@allianz.com
+33 158 858 863

Singapore
Wendy Koh
wendy.koh@allianz.com
+65 639 537 96

South Africa
Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 112 147 948

OUR EXPERTS

Michael Bruch
Head of Emerging Trends/ESG Business Services, AGCS
michael.bruch@allianz.com

Ralf Grosser
Partner of Allianz Consulting, Allianz Technology
ralf.grosser@allianz.com

CONTRIBUTOR CREDITS AND ACKNOWLEDGEMENTS

Michele Lagioia, an affiliate of the Italian Association for Artificial Intelligence

Allianz Consulting, Allianz Technology

Follow Allianz Global Corporate & Specialty on
Twitter @AGCS_Insurance and Linked In

www.agcs.allianz.com

Allianz Global Corporate & Specialty SE
Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany
Commercial Register: Munich HRB 208312

March 2018