Liberating Intelligent Machines with Financial Instruments

by

Anniina Huttunen[*], Jakke Kulovesi[**], William Brace[**], Lorenz G Lechner [***],
Kari Silvennoinen[**], Vesa Kantola[** *]

1.   Introduction

In science fiction, Isaac Asimov's three laws of robotics, as presented in his novel I, Robot, are the classical starting point for machine responsibility analysis.[1] Machine ethics research has widely followed Asimov's example[2]. Murphy and Woods[3] propose alternative laws inspired by Asimov's original laws that emphasize a developer's view on the ethics of robotics. In these works, machine responsibility is presented from the ethical point of view, but product liability issues are mostly absent, as is legal analysis. The present state of robot legal liability issues is to some extent described in existing literature.[4] This paper addresses responsible robotics from a legal perspective. However, instead of focusing on ethical considerations elaborated in philosophy and Artificial Intelligence (AI)[5] communities[6], the legal liability risks related to inherently error-prone intelligent machines are considered and a solution combining legal and economical components is proposed.

Because of the technological difficulties in creating perfectly functioning machines and the cognitive element inherent in intelligent machines and machine interactions, we propose a new kind of legal approach, i.e. a financial instrument liberating the machine. In this framework, a machine   can   become   an   ultimate   machine   by   emancipating   itself   from   its

---

[1] According to Asimov Law's
    1) a robot may not injure a human being or, through inaction, allow a human being to come to harm,
    2) a robot must obey orders given to it by human beings, except where such orders would conflict with the First Law, and finally
    3) a robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

[2] W. Wallach, "Implementing moral decision making faculties in computers and robots", AI & Society, vol. 22, no. 4, pp. 463-475, April, 2008. C. Allen, W. Wallach, I. Smit, "Why Machine Ethics?," IEEE Intelligent Systems, vol. 21, no. 4, pp. 12-17, July/Aug. 2006, doi:10.1109/MIS.2006.83. J. Gips, "Towards the ethical robot", in Android epistemology, MIT Press, Cambridge, MA, 1995, pp. 243-252.

[3] R. Murphy, D. Woods, "Beyond Asimov: The three laws of responsible robotics", Intelligent systems, vol. 24, no. 4, pp. 14-20, July/Aug. 2009.

[4] P. M. Asaro, "Robots and Responsibility from a Legal Perspective," in Proc. of the IEEE 2007 International Conference on Robotics and Automation (ICRA'07), Rome, April 2007. M.R. Calo, "Open Robotics" Maryland Law Review, vol. 70, no. 3, 2011.

[5] Artificial Intelligence is "the science and engineering of making intelligent machines, especially intelligent computer programs....Intelligence is the computational part of the ability to achieve goals in the world." John McCarthy,   Basic   Questions,   What   is   Artificial   Intelligence?   http://www-formal.stanford.edu/jmc/whatisai/node1.html

[6] N.E. Sharkey, "The ethical frontiers of robotics", Science, vol. 322, no. 5909, pp. 1800-1801, Dec. 2008, DOI: 10.1126/science.1164582.
    R.. Arkin, "Governing lethal behavior: embedding ethics in a hybrid deliberative/reactive robot architecture", ACM/IEEE international conference on Human robot interaction, pp. 121-128, March 12-15, 2008. J. Gips, "Towards the ethical robot", in Android epistemology, MIT Press, Cambridge, MA, 1995, pp. 243-252

manufacturer/owner/operator. This can be achieved through the creation of a legal framework around this ultimate machine that in itself has economic value.

We start this article by assessing the liability risks related to intelligent machines. Currently, the manufacturer or operator is held liable depending on the circumstances. Thereafter we will examine the management of the risks by technical and legal means, i.e. by means of liability stocks liberating the machine. The article relates to the European context. However, the solution can easily be adapted to other jurisdictions.

2.   Identifying and evaluating risk in intelligent machines

In this paper, the intelligent machine can be a robot, an artificial agent or other machine that implements some functions requiring autonomous decision making. Such a machine consists of the machine hardware, software, and an additional level of abstraction, the machine cognition. These three abstraction levels are used to look at the same entity from different perspectives. In reality, the physical machine hardware implements the software and similarly, the software implements the machine cognition. However, from a legal perspective, these levels have traditionally been understood to require separate considerations. Hardware can malfunction, break, or simply not fulfill its specifications, potentially causing harm. Similarly, software can have bugs, i.e. undesired features or non-compliance with specifications. These kinds of software problems can cause damage directly or through control over the hardware. In machine design, an ideal machine has both hardware and software that are error-free, disregarding the occasional need for maintenance and malfunction due to natural wear and tear. However, the third abstraction level, the cognition, lacks clear measures for perfect performance and thus causes problems from a legal perspective. With respect to human cognition, this imperfection is subsumed under the term "human error".[7] In contrast, intelligent machines are not yet given this acknowledgment of imperfection, i.e., we do not speak of "machine error" in analogy to human error.

Traditionally, the element of cognition is the starting point for speculation about robot rights. Since the early days of digitalization there has been an-ongoing debate over the idea of civil rights for robots.[8] Recently, a British Government Report anticipated a "monumental shift" in the area of robo-rights, once robots would become sufficiently intelligent.[9] While it is true that

[7] D. Woods, L. Johannesen, R. Cook, N. Sarter, Behind Human Error: Cognitive Systems, Computers and Hindsight. Ohio State University, Dec. 1994.

[8] R. Freitas Jr., "The Legal Rights of Robots", http://www.rfreitas.com/Astro/LegalRightsOfRobots.htm, Student Lawyer 13, January 1985, pp. 54-56.

[9] R. Beschizza, British Govt. Report Anticipates Rights For Artificial Consciousness. December 21, 2006. http://www.wired.com/gadgetlab/2006/12/british_govt_re/
        Robots could demand legal rights, 21 December 2006, http://news.bbc.co.uk/2/hi/technology/6200005.stm

courts have found robot judgment superior to human judgment in certain circumstances,[10] it should be pointed out that the capability of developing artificial intelligence is not connected to legal rights or duties. In other words, the ability to act rationally is not the deciding factor for granting rights to human beings. Even though robots can give humans orders that they are legally obliged to follow, like in the court cases mentioned earlier, they are still, like ordinary machines, considered the property of humans. However, the increasing use of sensory input in machines and the associated gain in autonomy and intelligent behavior is likely to lead to the need for robot liberation.

What is intelligence then? Here, the following definition is proposed: intelligence is an adaptation to complexity. Complexity can vest in the environment, the task, the dynamics of the world, or anywhere relevant to the agent or machine. In the presence of complexity, perfection is rendered impossible by the combinatorial explosion of different possibilities that should be considered in order to make an optimal decision. Intelligence is understood here as the art of managing complexity. Elaborating on the definition adopted above, the more complexity an agent can handle and the better it succeeds, the more intelligent it is considered to be. In the absence of perfect knowledge and inference, intelligence is about making good guesses in relative uncertainty. This observation is the main cause of "cognitive errors", i.e., when the guess is wrong, an intelligent agent is operating under false model conditions. Thus, an intelligent machine is inherently error-prone following directly from the definition of intelligence. Aside from this, there is another important factor relating to intelligence: since it is an adaption it has to be evaluated in its context. Outside the specific adaptation domain, intelligence is lost if new domains differ from the native one. Humans, for example, have a broad scope of intelligence, whereas the Deep Blue chess computer has only a very limited context in which it behaves intelligently.

Manifestation of intelligence in a machine or an agent can be divided into three main classes. First, the agent can be autonomously intelligent. In this case, a machine agent implements intelligent functions independently, without need for human intervention. Secondly, the machine can augment human intelligence, acting in tight interplay with a human. In this case intelligence is both borrowed from the human and created from human-robot interaction. Thirdly, intelligence can be analogous to swarm intelligence,[11] i.e., multiple robots can elicit complex and intelligent behavior when interacting together, even when any of the robots could be safely considered "stupid" in individual examination. Humans express all three origins of intelligence. We can operate independently or in complex social constructs like states and companies. In addition, humans adopt tools to augment their physical and mental capabilities. In the second case examined above, liability can often be attributed to the human operator. But

---

[10] In Klein v. U.S. (13 Av.Cas. 18137 [D.Md. 1975]). Wells v. U.S. (16 Av.Cas. 17914 [W.D.Wash. 1981]

[11] E. Bonabeau, M. Dorigo, G. Theraulaz, Swarm Intelligence: From Natural to Artificial Systems, Oxford University Press, 1999.

when the robot is acting independently or a group of robots is expressing complex behavior, attributing responsibility and liability becomes much more complex.

Naturally, the question occurs whether the relationship between a robot and owner is then similar to that of slave and dominus in ancient Rome? The superficial similarities are plentiful: slaves were forced labor enabling the productivity and wealth of society and, as such, normally had no rights, but were considered property of their masters. At first glance, this seems to correspond exactly to the relationship between humans and robots. However, there are some fundamental differences between the legal status of robots and slaves. Most importantly, with robots also the manufacturer has to be taken into account. While the robot is its owner's property, the manufacturer is closely connected to the use of the robot — at least, if the robot cannot be considered to operate like clockwork and damage is caused neither to humans nor property.

According to the Product Liability Directive 85/374/EEC[12] "liability without fault on the part of the producer is the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production." Product liability applies to defective or dangerous products (i.e. tangible products, e.g. services are excluded). Pursuant to the Product Liability Directive product manufacturers, distributors, suppliers, retailers and marketers can be held liable for injuries caused by defective products. Product liability is a category of so-called strict liability, i.e., the manufacturer can be held liable, even if, it did not act negligently, when manufacturing the defective product. Moreover, in the context of robot-related services (operators) the tort liability considerations have to be taken into account. In accordance with the law of torts, anyone who intentionally or negligently causes damage to another is liable to compensate said damage. Negligence in this context means carelessness that causes damage to another person or property.

From a legal point of view, it is important to keep in mind the distinction between situations where machines cause damage, i.e. product liability or tort liability, and situations where machines do not work as they should work, but damage is not necessarily caused, i.e. contractual liability. In Europe, the applicable directive in the first case is the Product Liability Directive (and national tort law principles in the context of robot-related services and in situations where the damage is caused to third parties), whereas the Consumer Sales and Guarantee Directive[13] and the Unfair Contract Terms Directive[14] are of relevance in the context of contractual liability. Liability is a prerequisite for the insurance framework.

---

[12] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210 , 07.08.1985, p. 29.

[13] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171, 7.7.1999, p. 12.

[14] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29.

3.   Risk Management

The first step in creation of a legal framework around this ultimate machine is to make applying for the insurance mandatory. However, not all machines need to be insured. In the following chapter we classify machines into different risk-categories, analogously using the classification of different vehicles in traffic (e.g. there is no duty to insure bicycles) in the Nordic traffic liability insurance system. The obligation to apply for insurance is based on the categories so created. At the same time, risk-profiling provides the necessary information for the market to estimate the price for the risk before actual statistical data becomes available. The second step is to allocate the risk to the market by means of liability stocks. The liability stocks can be compared to reinsurance practices.

3.1   Step 1 – Mandatory insurance for certain types of machines - setting design practices / risk-profiling

Managing risk is only possible, if the risks and associated factors are identified. We consider two main risk factors: predictability and damage potential. Predictability relates to how foreseeable the actions of a machine are. When the proposition of "intelligence equals to unpredictability" is accepted, the obvious conclusion is that from a predictability point of view simplicity - or even "stupidity"- is preferable over intelligence. A stupid machine that is well-designed and implemented is reliable and predictable according to clockwork logic. In contrast, even a well-designed and well-implemented intelligent machine carries the potential for errors and is unpredictable by nature. It is therefore essential to identify the machine's task and performance requirements in order to choose the level of required intelligence properly. Damage potential estimates the magnitude of material damage, and/or bodily injury the malfunction of a machine could cause. As a rule of thumb, the more physically powerful a machine is the more damage it can possibly cause. In addition, the environment in which a machine operates can dramatically increase its damage potential and needs to be taken into account.

Risk profiling is employed in order to assess the potential liabilities of autonomous machines.. Risk-profiling can be understood as a continuum of risk-reducing and risk-increasing factors that add up to a risk evaluation profile with the two dimensions of predictability and potential damage. The following presents some central factors to be considered in intelligent machine design:

Human presence: whether or not a robot is operating in relative proximity of humans. Are the humans in the robot environment trained to work with the robot or outsiders with no prior experience in dealing with the robot? What is the amount of human contact and interaction in normal operation? Unnecessary human contact should be avoided to reduce the potential risk of causing harm to humans, when the robot behaves erroneously.

Robot physical capabilities: what kind of physical manipulation is the robot capable of. The reach, strength, and speed of the robot is included. In addition, it includes the robot's physical

form as such - are there sharp edges or hard surfaces that can easily injure a human in unintended contact? The robot should ideally be designed so that damage caused in an accident or collision is minimized.

Robot connections and power over external entities: The extent to which the robot has external control. The power to control external forces is an important factor in increasing the potential for harm. An internet virus is a good example of a case where an intelligent agent has virtually unlimited potential for damage, should all things go wrong. Thus, keeping the connections limited and adding some hard firewalls or areas of hard boundaries to robot influence is a good practice in limiting the potential for harm.

Robot mobility: what kind of obstacles can it overcome and what is its operational range. How fast can the robot move? Robot mobility increases both its damage potential and its unpredictability. Precautions should be taken to prevent the robot from escaping from its intended environment, i.e., to prevent a hospital robot from accidentally wandering around in the streets. In addition, it is essential for the robot to be able to identify its dislocation and react accordingly. Restricting robot mobility can be of great help in managing the risk of a robot causing damage through its cognitive or physical errors.

Level of autonomy: how in/dependent is the robot The more autonomous the robot, the more difficult it generally becomes to predict its actions.

Robot learning and adaptation capabilities: how flexible and capable of learning is the robot. The more the robot can learn by itself and adapt to its surroundings and tasks, the more difficult it is to predict the robot's actions.

Connections to human infrastructure: the extent to which robots are integrated in infrastructure. Robots that operate as part of an infrastructure have the potential to create huge indirect harm. Should a traffic control robot malfunction, the potential for cumulative harm would be significant. This type of damage is different in nature from that in most of the other cases mentioned so far - instead of mainly causing additional damage, a infrastructure-critical robot or agent causes the loss of the benefit it creates and the benefit to which it has been bound. Thus, binding intelligent machines to human infrastructure greatly increases the potential for harm.

Connections to the natural environment: the extent to which robots are integrated into nature. Plant-eating robots have been suggested[15] and robots can have connections to our environment in countless other ways. Close interaction of the robot with the environment causes greater potential risks.

---

[15] Energetically Autonomous Tactical Robot (EATR) Project. [online]. available: http://www.robotictechnologyinc.com/index.php/EATR [Accessed: Sept. 26, 2009]

Self-replication and self-maintenance: the extent to which a robot is self-sustained. The more a robot can take care of itself, the greater the risk for harm and unexpected consequences. A self-replicating robot that has access to all the resources it needs has a carries huge potential for damage. Thus, capability to self-replicate should be considered costly with respect to both the potential damage and unpredictability factors.

The above factors are added up to give an estimated worst-case scenario, and an estimated normal-operational scenario for the sphere of influence of the robot or agent. For example, an autonomous mine-shaft car is limited in its influence to the shaft itself and its immediate surroundings, depending on the nature of the mine and the mobility-restriction techniques used. In contrast, the sphere of influence of an autonomous vehicle operating in the public road network is in the worst case limited only by its maximum cruising range. In a more abstract case, a power-plant optimizing agent has influence over entire continents in the worst case, and only its local electricity distributing domain in the most probable case. Next, the factors influencing potential for damage have to be added up in a similar way. In total, the robot's sphere of influence (reflecting uncertainty) is multiplied with its potential for damage, giving the final risk profile classification.

The obligation to insure should be set based on the above-mentioned factors. Moreover, the risk-profiling serves as a starting point for pricing.

3.2 Step 2 – Creating liability stocks

Traditional insurance business is based on quantifiable risks with large customer pools, so that annual variance is minimized and losses can be managed by adjusting the price of the insurance policy. One difference in comparison to the traditional insurance business is that smart machines are more prone to class-based malfunctions. Unlike fires and cancer, which are random, risks relating to smart machines are easier to quantify on the basis of historical data and the amount of annual occurrences can be forecasted. However, such information may not be available for intelligent machines due to their fast innovation cycles. Further, a fire at one type of a house does not mean similar houses will burn down in the near future. In this respect intelligent machines are more comparable to modern operating systems with which it can be anticipated that if one version is vulnerable, all other versions will be vulnerable as well. Airplanes are a good example of class-based malfunctions and how they are managed today. An incident with certain model of an aircraft causes investigations and repair work on all aircrafts of the affected model. This is possible, because of the extensive certifications and paperwork kept on all aspects of an aircraft's lifecycle, e.g. repairs.

One major challenge in creating a financial instrument for smart machines is transforming uncertainty into a quantifiable risk. As described in Step 1, one way to achieve this is through risk profiling. Having a quantifiable risk is important for proper pricing of financial instruments.

An alternative way to cover one's exposure to risk is through the financial markets. It is likely that at first, liability stocks will be "exotic" financial instruments. It may be difficult to build a model to quantify the risks related to a class of machines due to the lack of historical information. Statistical models are hard to build without any historical information.[16] Therefore the first machine insurances may be expensive from the buyer's perspective, because of the perceived risk and non-liquidity of markets. The counter-parties are most likely to be large reinsurance companies, investment banks or hedge funds, which are capable of handling such risks (Fig 1).

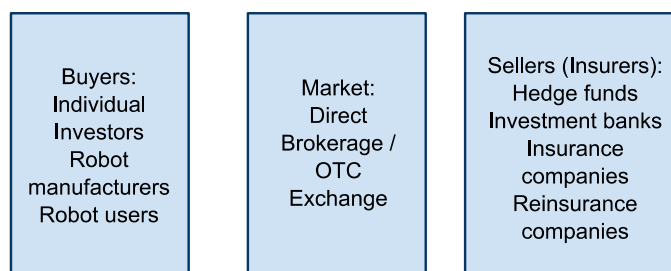| Buyers: Individual Investors Robot manufacturers Robot users	Market: Direct Brokerage / OTC Exchange	Sellers (Insurers): Hedge funds Investment banks Insurance companies Reinsurance companies

Figure 1: Players in the ultimate insurance machine liability stocks model

Reinsurance companies are traditionally used by insurance companies to manage their risks better. Certain risks (e.g. earthquakes, extended droughts) have a very low probability, but if the risk actualizes, the damage will be too high for any single insurance company to cover. Similarly, in case of a new product, like machine insurances, a single insurance company may not have the expertise in such a specialized risk, and therefore might transfer the risk to a reinsurance company instead.[17] Such reinsuring may be most suitable for robots that are most vulnerable to class-based risks. However, as to earthquakes and nuclear power plants, if the worst scenario materializes, monetary compensation is not enough to cover the damage. This shows the limits for risk management what insurance can provide.

Robot-related liability stocks are comparable to reinsurances. As with traditional reinsurance models, the risks are transferred to the individual investors buying the stocks, and do not remain with the reinsurance companies. Alternatively, the liability stocks could also be directed to manufacturers. Moreover, in another model the government could also be a buyer of these stocks. Government could play a crucial role to provide the necessary liquidity for liability markets to function properly, acting as a sort of a "counterpart-of-last-resort".

It is worth mentioning that the insurance constellation could be compared to a limited liability corporation (approved in England in 1856). In the 18th century, the Lord Chancellor of Great

---

[16] Compare with Nordic traffic liability insurance systems. This will be elaborated later with references to e.g., E. Routamo, Liikennevahinko (1967).

[17] P. Li, M. Shaw, K. Stolarick, and K. Wallnau, "The potential for synergy between certification and insurance", International Workshop on Reuse Economics in conjunction with ICSR, 2002.

Britain[18] remarked about corporations that they "had no soul to damn and no body to kick" and were therefore hard to hold accountable for misdeeds. The same thing will probably apply to intelligent machines. While they have a "body to kick", kicking will not do much good, as they still lack a soul to damn. As noted previously, the insurance constellation could also be compared to the Nordic traffic liability insurance systems.

The liability stocks constellation could also be seen as an indemnity obligation. Indemnity obligations have their origin in the Anglo-American contracts tradition. It is a contractual obligation used to transfer liability between the contracting parties. Thorpe and Bailey[19] define indemnity clauses as follows: "An indemnity is an undertaking by one party to meet a liability which would otherwise fall on the other." The condition of indemnity is expressed in general with words like "indemnify and to hold harmless". An indemnity obligation is a specific performance obligation, which is based on an agreement. It does not correspond to tort liability, but is approaching liability insurance, or first demand conditions in a warranty. This is the same type of payment obligation as damages paid to the customer based to the insurance.

3.3 Case: Liability for erroneous software

Liability for erroneous software is a negative example, where the current liability regime fails to provide proper guidance. Again, it is important to highlight the distinction between machines, which do not work as they should work according to the contract and machines which cause personal injuries or damage to property. What effect would it have if the scope for the insurance framework would be extended to the liability risks relating to contractual defects? Then at issue would not only be damages to property and persons, but the product itself would also covered.

Currently, the issue under debate in European Consumer Policy is not the product liability legislation, but the directives on contractual liability between a seller and a consumer. The debated issue is whether the scope of the Consumer Sales and Guarantee Directive should be extended 'to include intangible goods, such as software and data', as the loophole in the legislation is considered a 'potential consumer protection lacuna'.[20] Currently, consumers are

---

[18] J. Coffee, Jr., "'No Soul to Damn: No Body to Kick': An Unscandalized Inquiry into the Problem of Corporate Punishment," Michigan Law Review, Vol. 79, No. 3 (Jan. 1981), pp. 386-459.

[19] C. Thorpe & J. Bailey, Commercial Contracts. Kogan Page Limited: London 1999.

[20] Green Paper on the Review of the Consumer Acquis (COM(2006) 744 Final

  M. Loos, "Consumer Sales Law in the Proposal for a Consumer Rights Directive". European Review of Private Law, Forthcoming; Centre for the Study of European Contract Law Working Paper Series No. 2009/07. Available at SSRN: http://ssrn.com/abstract=1425036

  A. Huttunen, V. Oksanen, J. Laine, "Digital Consumer and User Rights in EU Policy", ACM International Conference Proceeding Series; Vol. 342. Proceedings of the 10th international conference on Electronic commerce Innsbruck, Austria. SESSION: SemWeb/EGov table of contents. Article No. 30 Year of Publication: 2008.

left without proper protection when they buy software In contrast, embedded systems, such as robots, are included in the normal consumer protection legislation.

Naturally, the business sector, including digital service providers, is against the extension of liability.[21] According to them e.g. "It very much depends on the way the consumer installs the software on his computer, and whether or not he/she was aware or not at the beginning of the compatibility of the service with his/her own material." Moreover, "There are many different parts that interact with each other but are not necessarily always compatible according to the quality of the product, the "age" of the computer, or the other software/ hardware installed. Contributors indicated that if there is a malfunctioning of the digital product supplied, it would be extremely difficult to determine which one of the elements caused the damage."

Those arguments were used in the context of a review of consumer *acquis* on consumer law issues related to consumer sales. The Review of the Consumer Acquis does not cover product liability. It seems, however, that the arguments could be used as a motivation for the insurance machine also when it comes to product liability issues. Lately, the debate has concerned software, music and games, which do not work as they ought to, even though they typically do not cause damage to anyone. However, due to the emergence of intelligent machines the product liability issues are likely to become topical. We most definitely do not want to end up with the same problems we have with software liability, when it comes to robots that are capable of doing much more than just deleting our pictures, music, and documents.

3.4   The new intelligent system development approach

Through intensive research activities, we are standing at the edge of a new renaissance in science and technology. This is substantiated by an understanding of the structure and behavior of matter from the nano-scale up to the complex system of the human brain. Science began its separation from philosophy two centuries ago, but at present there is an ongoing unification of science based on unity in nature.[22] For a complex machine to serve society in an efficient way, the unification with nature should be accompanied with a new risk-management tool. Holistic investigation of this unification leading to the technological and risk-management convergence and thus a more sophisticated machine is inevitable. Rapid advances in convergent technologies have the potential to enhance both machine performance and reduce the strain of the natural world on elements, but so far do not address liability issues.

---

[21] Preparatory Work for the Impact Assessment on the Review of the Consumer Acquis - DG HEALTH AND CONSUMER PROTECTION - Analytical Report on the Green Paper on the Review of the Consumer Acquis submitted by the Consumer Policy Evaluation Consortium. (06/11/2007). Available at: http://ec.europa.eu/consumers/rights/detailed_analysis_en.pdf

[22] M. Roco, W. Bainbridge, Converging Technologies for Improving Human Performance, Springer, Apr. 2003.

Innovative advances are blurring the interfaces between the previously separated fields of science and technology. Development in system approach, through the use of systems engineering processes in conjunction with convergence technology allows for a thorough understanding of the natural world.[23] Human performance is included in design approaches to improve human behavior and to reduce accidents caused by humans. Likewise, legal responsibility should be analyzed and included in design approaches. New Product Development (NPD) is the term used to describe a recent complete process of bringing new products involving integration of business and engineering, to the market.[24] There are two parallel paths involved in this approach: one involves generating the idea, product design and detail design and the other involves market research and marketing analysis. We propose a new approach, the New Intelligent System Development (NISD) to converge engineering design, business/market practices, legal and financial practices to bring an ultimate machine to the market. Thus, instead of two parallel paths, as proposed in NPD, there will be three parallel and integrated parts (Fig. 2).
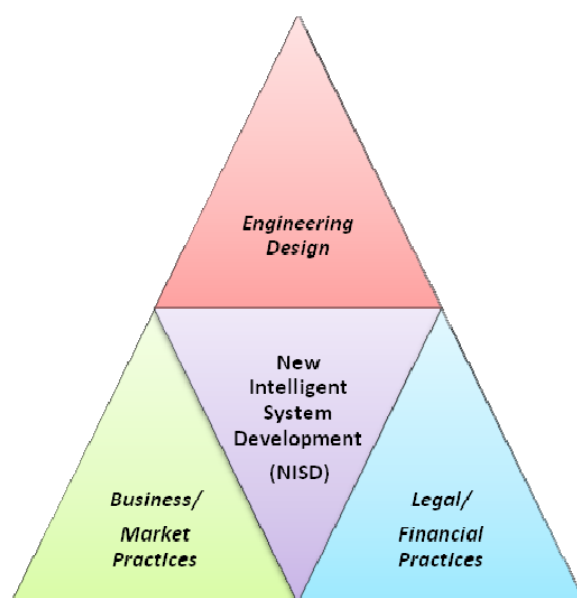
Figure 2: The NISD approach with interacting parts

[23] Pahl G. and Beitz W. *Engineering Design. A Systematic Approach 3rd Edition.* 2007,Ken Wallace, Luciënne Blessing, translators and editors. (Springer, Berlin-Heidelberg).
    Blanchard B., Fabrycky W. (2006) Systems engineering and analysis 4th edition. Prentice hall
    INCOSE SE Terms Glossary Version 0 October 1998 Copyright (c) 1998 by INCOSE.

[24] Husig, S; Kohn, S; Poskela, J (2005). "The Role of Process Formalisation in the early Phases of the Innovation Process". 12th Int. Prod. Development Conf. Copenhagen.

In existing design processes, business analysis and market analysis is parallel to the design process.[25] In the NISD approach, the business/market analysis and the legal/financial practices will be integrated in the design process right from the conceptual design phase. Engineering design is a challenging activity, because it deals with largely unstructured problems that are important to the needs of society. The first fundamental canon of the ABET Code of Ethics states that "engineers shall hold paramount the safety, health, and welfare of the public in the performance of their profession." Even though a similar statement has been presented in engineering codes of ethics, since the early 1920s, society has increasingly participated in enforcing good engineering practices.[26] The major social forces that have had an important impact on engineering practices are occupational health and safety, consumer rights, environmental protection, the freedom of information and public disclosure movements. These have led to several regulations, which have been adopted right from the conceptual design phase as constraints on the design. In our proposal, insurance contract practices should be added to the social forces.

The subsequent regulation will influence engineering practice in the following ways:

- Greater influence of lawyers on engineering decisions
- Greater influence of the financial market in engineering design
- More time spent in planning and predicting the influence of the financial market and future effects on engineering projects
- Increased emphasis on "defensive research and development", which is designed to protect the ultimate insurance machine against possible litigation
- Increased efforts expended on research, development, and engineering to create a legal framework around the ultimate insurance machine which in itself do not directly enhance corporate profit, but can affect profit in the financial market

The conceptual design includes a system design specification (SDS), which serves as the basic control of and reference for the design and manufacturing of the system. Thus, the insurance regulation is included as an element of SDS. The intelligent system will go through a cycle from birth, into an initial growth stage, into a relatively stable period, and finally into a declining state that eventually ends in the retirement of the system (Fig. 3).

---

[25] Husig, S; Kohn, S; Poskela, J (2005). "The Role of Process Formalisation in the early Phases of the Innovation Process". 12th Int. Prod. Development Conf. Copenhagen.

[26] Dieter, G., and Schmidt, L.C., 2008, Engineering Design" McGraw-Hill, New York, NY.
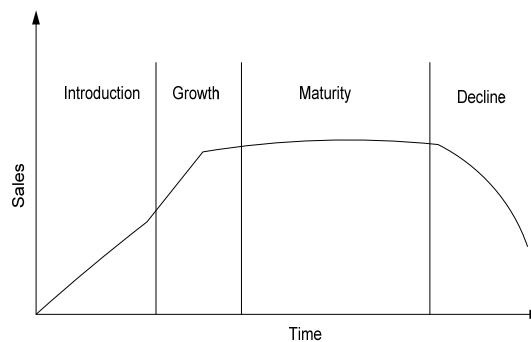
Figure 3: Intelligent system life cycle

Looking more closely at the system life cycle, we identify that the cycle is made up of many individual processes (Fig. 4). In this case the cycle has been divided into the pre-market and market phase. The former extends to the conceptual phase and includes the research & development and the marketing studies needed to bring the system to the market phase. The investment (negative profit) needed to create the intelligent system is shown along with the profit. A financial market studies is added to the life cycle process as shown in Fig. 4. This will span across the two phases (pre-market and market) starting from a market study in the pre-market phase and continuing in the market phase. This brief discussion serves to emphasize that the NISD approach, which leads to an ultimate insurance framework, is a complex, costly, and time-consuming process, but it will help to emancipate the machine and create a new kind of financial instrument.
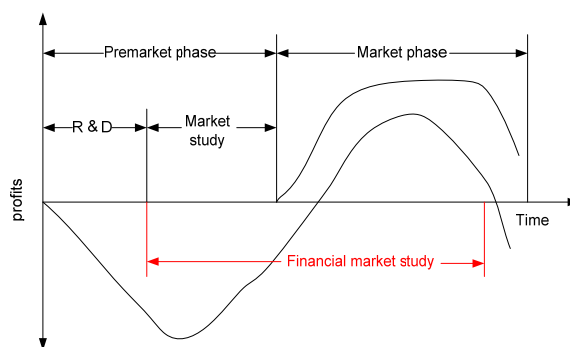

Figure 4: Expanded intelligent system life cycle with financial market study

4.   Conclusion

The development and use of intelligent machines faces tremendous challenges in current legal systems. Technological development is stifled by liability risks. Currently, the manufacturer or operator is held liable depending on the circumstances. Due to both the technological limitations for perfectly functioning machines and the unpredictable cognitive element, intelligent machines are not perfect and it is almost guaranteed that there will be failures causing harm. However, this

is not an excuse not to aim for failure-free operation. Instead, the inevitable failures should be managed so that present economical or legal issues do not hinder the potential human development and prosperity enabled through the adoption of new technologies.

We propose a new kind of legal approach, i.e. the ultimate insurance framework, to solve the related legal and economical difficulties in order to support the technological pursuits. In the insurance framework, a machine can become an ultimate machine by emancipating itself from its manufacturer/owner/operator.. This can be achieved by creating a legal framework around this ultimate machine that in itself has economical value. The first step in creation of a legal framework around the machine is to make applying for the insurance mandatory. The obligation to apply for insurance is based on risk profiling created in this paper. Similarly, this article makes an attempt to include legal responsibility in design approaches. If machines are considered legal persons, they can be considered items having rights and duties. Interestingly, this Insurance Machine Constellation does not make it necessary to decide, whether robots or software agents have to be treated as legal persons.

Currently, there is an ongoing debate in Europe on the idea of extending the Consumer Sales and Guarantee Directive to software. This is a contract law issue. Because of the advent of autonomous intelligent machines, it is likely that a discussion on product liability issues will follow. Presently, robots as embedded systems are included in the normal product liability scheme. However, issues related to robots as services, and the liability division between the manufacturer and operator/owner, may become topical, as there is no specific legislation covering the area. Moreover, even if the product liability and tort law scheme was considered as sufficiently extensive, a new approach on the allocation of liability is needed, both from the manufacturers' and consumers' point of view.