Transdisciplinary Engineering: Crossing Boundaries
M. Borsato et al. (Eds.)

doi:10.3233/978-1-61499-703-0-15

Managing Risks in Knowledge Exchange: Trade-Offs and Interdependencies

Nel WOGNUM[a,1], Mark WEVER[b] and Josip STJEPANDIĆ[c]
[a]*ISPE advisor, Zeist, The Netherlands*
[b]*Financial consultant, Brazil.*
[c]*PROSTEP AG, Darmstadt, Germany*

Abstract. Knowledge exchange, as required in Trans-disciplinary Engineering processes (TE) is not without risk. Many types and sources of risk exist, which depend on the type of interdependency between actors (companies) in TE teams as well as on the strategic nature of the knowledge exchanged. Risks need to be managed, not only with technical means, but also with other types of methods, like contracts. In this paper, different types of interdependencies are described which influence the risks that actors may encounter. Moreover, in managing risks, different trade-offs arise, which complicate the choice of a suitable method. In the paper, an introduction to different types of contractual solutions is presented, which need to be extended in further research.

Keywords. Trans-disciplinary Engineering, Knowledge Exchange, Intellectual Property

Introduction

Trans-disciplinary Engineering (TE) is a logical consequence of the concept of Concurrent Engineering. It more closely emphasizes the need for different disciplines to collaborate across intra- and inter-company borders. Such collaboration already starts with the conception of an idea until the release of the product for production and service. Destruction or take-back for recovery also need to be taken into account during the TE process. Not only engineering disciplines are involved in collaboration, but also marketing, production, maintenance and service, sales, and representatives of end-user communities, including legal and financial entities. TE as such is an encompassing concept, requiring extensive technical and organizational solutions for making it work.

A complex concept like TE is difficult to implement in practice. It takes many years to take the necessary steps to master the many challenges that accompany TE (see amongst others [1]). There are also many trade-offs to be made because, for various reasons, optimization of products, processes and organization is often not possible. First of all, legislation of the different countries involved may inhibit optimal ways of working. Second, people may inhibit optimization because of differences in cultures and working habits. Third, the openness between departments and companies as required in optimal TE may endanger company assets, especially valuable knowledge assets. This last point will be the subject of this paper. We will discuss the potential

[1] Corresponding Author, E-Mail: wognumnel@gmail.com

risks of TE with respect to knowledge exchange, as has been discussed before elsewhere [2]. We propose contractual solutions for managing the risks of knowledge exchange as is needed in the design process. Contracts in this context refer to both formal and verbal contracts, as well as investment-based contracts, like equity alliances or vertical integration [3].

The paper is organized as follows. In section 1, the history of CE towards TE is briefly described. Section 2 discusses in more detail the problem with free knowledge exchange as is required in TE. In section 3, a framework of contractual solutions is presented for managing risk in transactions between companies [3]. The framework is a proposed extension of the Transaction Costs Economics framework (TCE) of Williamson [4]. We will discuss possible contract forms for managing risks in knowledge exchange. Section 4 contains a summary and ideas for further research.

1. TE follows CE

In this section a brief history of CE is presented (section 1.1) as well as an explanation of the concept of TE (section 1.2).

1.1. Brief history of CE

The concept of Concurrent Engineering (CE) has been developed in the early 1980s. Initially, the emphasis was on the parallel execution of design and manufacturing processes to limit the number of design failures later in production. The notion of concurrency has been valid until now. Gradually, the emphasis has shifted to collaboration, because collaboration and teamwork is deemed crucial, especially because also the number of disciplines involved has gradually grown, while also the intra-company focus has been extended into an inter-company focus. In the early stages of CE the design had to take into account the manufacturing and production phases. Later, the whole lifecycle of a product became important in the design phase, including the idea development and after-sales activities like maintenance and repair and also asset recovery. Users, consumers, and other stakeholders, play a role now in current CE.

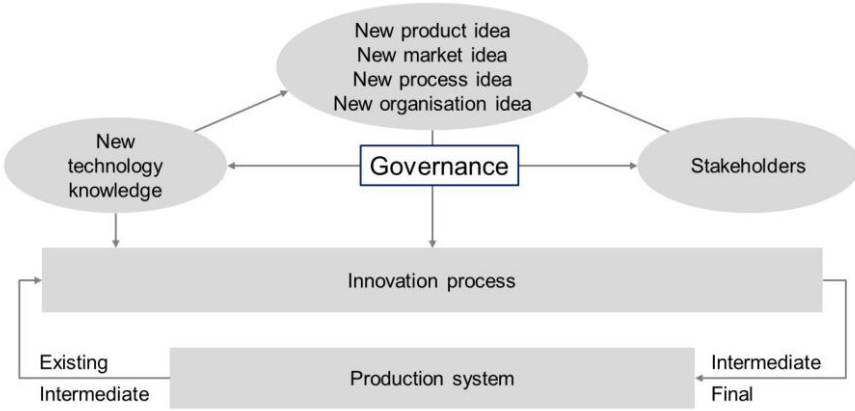

Figure 1. The system of CE [Wognum and Trienekens, 2015].

In Figure 1, the whole trajectory of CE is depicted [1]. In this figure, the start of a CE process is a new idea, possibly based on new technology or created with the help of stakeholders. The new idea can be a product, market, process or new organization idea or two or more of these together. The CE process, which can also be understood as an (open) innovation process needs to be governed by means of a suitable organization and organizational arrangement like teams, procedures, and mutual agreements between the stakeholders. The figure also emphasizes that the intermediate and final outcome of a CE process is a production system that is aimed to produce the intended products and/or services. The production system can be new, for example a new company or supply chain, but can also be an existing one, adapted for the new product.

1.2. From CE to TE

The concept of CE is characterized by a focus on customer requirements and embodies the belief that quality is a result of continuous improvement of a process [5]. Teamwork, as has been indicated above, is central to this approach. Teams may be at geographically different, networked, locations. This fact complicates CE because many different cultures, values, disciplines, functions, and technologies need to be aligned. CE is these situations, which more predominantly exist today, can be characterized as Trans-disciplinary Engineering (TE).

To achieve integrated, parallel, product and process design strategies, logistics, and functions need to be aligned as is indicated in Figure 1. Advanced information management systems are needed for enabling and supporting such integration. Such systems support intra- and inter-company collaboration and enable exchange of knowledge in the form of product, process and service models.

An example of a platform for information management for TE is SORCER [5]. Platforms like SORCER are able to support alignment of different proprietary information systems and exchange and processing of product models. In the next sections we will discuss some issues that accompany the exchange of models and knowledge, which constitute often the intellectual property of companies involved.

2. Trade-offs in knowledge exchange

A large part of intangible assets like knowledge of new technology and complex product models that are valuable for a company is called Intellectual Property (IP). Intellectual property is a broad label for the set of intangibles owned and legally protected by an enterprise from outside use of implementation without consent [2]. It consists of the business know-how (product, process, service) and rights (patents, trade secrets, copyrights and trademarks) [6]. Together these assets can be more valuable than companies' tangible assets.

The extensive exchange of knowledge through information systems is a feature of well-implemented TE [2]. It provides high transparency of processes, models and data, but as such forms an additional threat for the safeguarding of IP. Incidents are reported, such as product piracy, plagiarism, counterfeits, theft of data, and cyber crime [7]. It is, however, often difficult to identify violation of IP because of differences in political systems, organizational and technical constraints, and socio-economic situations [8].

Protection of IP in a TE world requires measures that take into account:

- The measures to be taken at each site [2],

- Integration of these measures into the overall product lifecycle management [2][9],
- Dependencies between companies in network or supply chain involved (see section 4) [3][10].

Some trade-offs need to be considered in managing risks in IP protection [2]. First of all, companies may have local competitive advantage, which they may loose when they 'go global'. A typical example is a supplier who participates in bidding for a concept solution for a new customer (OEM) in a country with low legal protection against IP violations, where the customer can easily distribute all knowhow presented by bidders to the bidder with the best commercial conditions (e.g., the lowest price). The local bidders can heavily learn and upgrade their know-how by participating in such a competition. However, local politics may prevent them from doing so. Second, social media make it extremely more difficult to restrict the free exchange of knowledge. Third, a choice needs to be made between the degree of policing and the degree of sharing. Fourth, it is not easy to decide which data are confidential and which are public. Fifth, costs of implementing measures against potential violation must be balanced against potential losses. Fifth, when multiple risks can be encountered, as is often the case in TE processes, a trade-off needs to be made for which risk to manage.

Stjepandic et al. [2] have described some technical approached for managing risks. For example, an OEM would allow the use of rich clients of their PDM system only at the supplier site. In this way, secure access is realized to the OEM's engineering database because of standardized processes like authorization and authentication of single users and devices. However, integration between the systems involved is prohibited in this way leading to large data queues at the supplier site.

Another technical approach is the management of patents. A patent is an IPR granted with exclusive rights for commercialization and can potentially bring huge benefit to an enterprise. Management of patents is aimed at reducing the risk of infringement. A variety of management approaches exists. Patent infringement analysis should be conducted frequently during a patent lifecycle. Suitable IT systems support this analysis, such as systems based on patent ontology engineering [2].

Protection of product data is another measure that can be taken. Artificial Intelligence (AI) offers techniques for improving CAD systems and PDM systems. AI covers methods for acquiring, processing and storing of knowledge. Knowledge-Based Engineering (KBE) technologies can be embedded in CAD and PDM systems. Embedded systems enable interaction of comprehensive product-specific knowledge and know-how in a single model. To manage risks associated with misuse and loss of models, the flow of knowledge has to be controlled in a predefined and traceable way.

Reverse engineering is another threat for misuse of IPR. One of the action fields of IPR is to disable this route.

In the next section a framework for risk management is discussed, which has been developed in the context of transactions between actors, which can be traders, different companies in a network or suppliers and customers in a supply chain.

3. A framework of contractual solutions

Companies, supply chains, business networks and economies have become more interdependent. as shown by the 2007-2008 financial crisis [3]. Insufficient monitoring of the actions of individual companies or actors has led to the bankruptcy of banks and

other financial institutions [3]. In TE environments protection of intellectual property rights (IPR) requires attention, because violation of IPR may cause not only much harm to the owner company, but also to all companies in the network or supply chain that are dependent on the results of a TE process.

In the next section, various types of interdependencies are specified and discussed. Differences in interdependency expose actors to different sources of risk. In the subsequent section three possible risk management strategies are discussed. The discussion is based on a framework for risk management that has been developed as an extension of the Transaction Cost Economics (TCE) framework [3; 4; 11].

3.1. Dependencies between actors in a TE process

In a TE environment companies are related in three basic ways: pooled, sequential, or reciprocal [12]:

- Companies in a pooled interdependency are relatively independent to each other, but share a common resource, like a financial resource, or a service provider. Misbehaviors by one of the members of the pool may damage the working of the pool by lost image and reputation. Conversely, when the resource is unavailable or produces low quality, all members are affected;
- Companies in a supply chain have sequential relationships. The output of one company is input for another. Often the receiver of the output cannot proceed when the supplier has not finished its output;
- Companies with reciprocal relationships can be found in networks that collaboratively work in a product development project. These companies depend on each other's input and output.

In a product development process, companies may be related in more than one way. For example, companies in a network with reciprocal relationships may also have sequential relationships. This is the case, when also manufacturers are involved in the network, which is certainly true for TE projects. In addition, service providers may be involved in a TE process, because of the information management infrastructure that is used, providing the companies involved with a pooled relationship. In the aerospace industry or in the food industry, quality management institutions may exist that act as a resource pool, which monitors behavior of individual companies in the network and may prevent bad actors from participating in the network.

In Figure 2, a situation is depicted of an OEM that participates in a TE network for the development of a new product, process, or service. It collaborates with its main supplier. OEM could tie its supplier to the collaboration with a strict contract in which it prohibits the supplier to use the results for other OEMs. Conversely, the supplier could protect its own knowledge from misuse by OEM. OEM also collaborates with a technology start-up that has developed alternative technology. OEM could decide to horizontally bind the start-up so that it becomes part of OEM. In this way leakage of knowledge is basically avoided. A service provider may play the role of service pool for the network. For each actor in the network specific authorizations are installed. A certification body is another pooled resource, for example, when the network wishes to develop a new product and process that satisfies strict environmental rules.

As indicated above risks taken in one place of the network or supply chain may affect other parts of the network or supply chain. Although pooled interdependencies seem the least intensive form of relationship, damages to a shared pool of resources will affect all actors [3; 13]. Collective action, such as a quality management body, is

needed to prevent such harmful outcomes, as there is little that individual actors can do to prevent such outcomes.

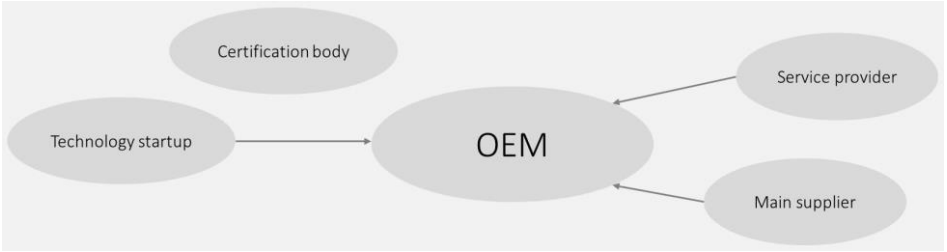

Figure 2. A possible configuration of a TE network with contracts

In sequential relationships, risks taken in one place of the supply chain may affect other parts. An example is the so-called bullwhip effect, where the increase in demand-order variability for upstream stages is due to decreasing insight into (final) demand information [14; 15]. In a TE environment, knowledge use in the manufacturing phase may create the risk of violation of IPR of another company that provided this knowledge in the development phase.

Reciprocal interdependencies are the most intensive. Actors heavily rely on each other, although risks may not be equally harmful to actors in the network. Nevertheless, the risk of strategic, self-interested behavior may decrease when interdependencies become more reciprocal. However, when circumstances change, actors need to put much effort in mutually adjusting themselves. In such cases effects may be amplified.

Risks are often associated with the degree of asset specificity, including high investments in technology needed for the TE process. High asset specificity ties actors to the network or supply chain, while it makes them more vulnerable to changes in the environment. In addition, the degree to which actors can monitor and measure behavior of other actors also influences the risks actors may encounter, like shirking (falsely claiming compliance with conditions) or opportunism (renegotiating conditions of the collaboration).

3.2. Risk management strategies in a TE context

In TE processes actors may have multiple interdependencies with the other actors participating in the process, making them vulnerable to multiple sources of risks. Trade-offs arise in deciding which sources of risk require the most attention, taking into account the costs of implementing suitable solutions, like contracts, to reduce the odds of the risk occurring or its impact.

Risks can be defined as the possibility of a harmful event (cost or loss) [16; 17]. In this paper the focus in on transaction of knowledge (product, process, and service models) as is needed in a TE process. Uncertainty may exist about the nature of the event or about the frequency of occurrence.

Three options can be distinguished [3] for managing risk:

1. Obtaining information to reduce uncertainty about the expected frequency or nature of the event;
2. Affect the probability that event occurs or affects the actor;
3. Minimize the impact when the event occurs.

The main risks that have been examined in the TCE framework are related to the strategic, self-interested behavior of actors, such as opportunism or shirking (see [3;

11]). Such behavior is possible because contracts are never complete: they always contain gaps and omissions. Information processing limitations [18] hamper actors' ability to anticipate and specify all possible situations or contingencies that may arise. In addition, a further risk is that actors in pools, networks, or supply chains may not be able to adapt when circumstances change, i.e., the risk of maladaptation.

Risks associated with opportunism are largest when actors have heavily invested specifically for the collaboration in which they act. This investment ties the actor to the collaboration. Risks associated with shirking are largest with high levels of performance measurement difficulty, referring to the extent to which an actor can measure the benefits and costs other actors bring to the collaboration. Risks associated with maladaptation are largest when collaboration is characterized by high uncertainty. High uncertainty refers to unanticipated changes in the environment of the collaboration (see [3]).

Wever et al. [3] describe four different manners in which contractual solutions can be used to manage risks. Although based on a supply chain context, these solutions are assumed applicable in a wider context, like TE.

First, actors can use contracts to minimize or reduce their risk exposure in collaborations. One way is by implementing hierarchical types of contracts, with legally binding safeguards. Such safeguards reduce the ability of actors to renegotiate conditions once specific investments are made. Moreover, the use of these contracts reduces the risks of shirking, by increasing actor's ability to monitor the other actors' performance. An example is a temporary virtual organization with legal contracts between actors.

Second, contracts can be structured in such a way that actors' incentives to act opportunistically or shirk are minimized. Sharing exposure to risk is a one way to do this. Mutual dependency of actors is a key aspect of risk sharing. Important for this strategy is that asymmetries between actors are reduced. When actors have made investments for the collaboration, they have committed themselves to the collaboration and thus have a stake in possible success. Conversely, they share the risk when outcomes are not successful.

Third, contracts may also be used to alter risk exposure, as when an actor swaps one type of risk for another. For example, as when contracts with strict conditions reduce the risk of opportunism, but at the same time increase the risk of maladaptation when actors operate in highly uncertain environments. Then, the actor's risk exposure has been altered from exposure to opportunism to exposure to maladaptation.

Fourth, risk can be transferred to or absorbed by other actors in the collaboration. In this case, 'the holder' of a risk has changed. For example, as when the exposure to price uncertainty is transferred from one actor participating in the TE process to another actor (e.g., by means of a fixed price contract).

The risks to which actors are exposed depend on the various dependencies they have with other actors in the TE process and how strong these dependencies are. For an OEM, with a strong incentive for undertaking the TE process, because of the high returns expected when successful, opening up its proprietary knowledge in the collaboration may be very risky. It may create a virtual organization with proper safeguards in which other actors participate that share the risk by opening up their proprietary knowledge in the collaboration. The risk of theft or counterfeit might then be reduced. The potential manufacturer of the envisioned end product could be part of the virtual organization or may even be vertically integrated with OEM to reduce uncertainty with respect to strategic behavior. However, proper safeguards need to be

installed for the suppliers of the manufacturer depending on the type of products they deliver to the manufacturer. For commodity type suppliers, relatively simple, but strict contracts are likely to suffice. For strategic suppliers more complex, but elastic contracts are usually needed.

However, note that in a virtual enterprise fundamentally opposing interests may exist of the actors involved. OEM commissions its suppliers or external service providers to provide components or explicit services. In principle, OEM is interested in the whole of technology and know-how resulting from the collaboration. Suppliers, on the other hand, may complain that draft designs they deliver to OEM in the concept definition phase were given to their competitors in a later phase. Similarly, suppliers may want to use the developments of one project for another project with another OEM. In this case, the first OEM is the financer and client of the new development, but at the same time supports indirectly its competitors without proper safeguards.

A list of contractual risk management strategies in a TE context is shown in Tab. 1.

Table 1. Examples of contractual risk management strategies in a TE context.

	Risk minimizing	**Risk sharing**	**Risk altering**	**Risk transferring**
Risk exposure ex ante	OEM has developed proprietary technology that its main supplier could appropriate and use in transactions with other OEMs.	OEM is investing in technology that could become the industry standard. It runs the risk that it fails to become widely adopted.	A spot-price contract is in place between a component supplier and OEM. The latter is exposed to the risk of price increases for the components, while the former to the risk of price decreases.	OEM runs the risk of losing a large amount of money when the product development project fails due to bankruptcy of its partner
Contractual intervention	OEM integrates the supplier into its operations.	OEM enters into an alliance or joint venture with another OEM.	The parties swap the spot-price contract for a fixed-price contract.	OEM can enter into an insurance contract with an insurance company
Risk exposure ex post	By taking-over the supplier, OEM has reduced the risk of misuse of its technology.	The risk of product failure is shared amongst the two OEMs	OEM is exposed to the risk of decreases in the price of the components (as it will have locked in a higher price), and the latter to the risk of price increases (as it will have locked in a lower price).	The risk of failure is transferred to the insurance company

At least, in defining suitable measure for managing risks, direct costs and opportunity costs need to be distinguished which can be ex-ante costs or ex-post costs [3].

3.3. An example of a technical solution

Each OEM (receiver of goods or services in a supply chain) is interested to outsource as much work and as little knowhow as possible to its suppliers. In case of a significant amount of sensible product data to be exchanged, just two alternatives exist: the suppliers may access these data at the OEM's site (which is difficult to implement from physical distance) or the OEM implements a comprehensive data exchange solution, which provides a significant level of protection for both parties.

A frequently used scenario is Engineering Change Management, which occurs in the later phase of product development, the production and service phase of the product lifecycle. A typical solution to manage data exchange in this scenario is shown in Figure 3.

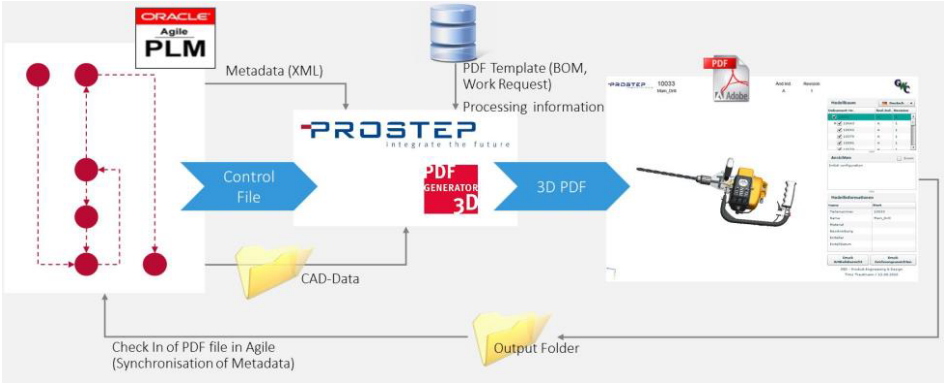

Figure 3. Data exchange to supply chain controlled by data extent and policy

An OEM (at the left side) deploys a comprehensive PDM system for product data management. In this scenario, a subset of necessary data is built by using an intelligent template with 3D PDF models. CAD data are translated to 3D PDF including product-manufacturing information (PMI) and embedded in the template [19]. Meta-information is stored in the template itself that may have several restrictions in access (time period, user or machine). The supplier can use low-cost software to insert his comments. In this way, the risk of data loss or unauthorized access is reduced to a minimum, allowing a stable and reliable communication.

4. Summary and further research

In this paper TE has been described as a concept in which multi-site, multi-disciplinary and multi-functional teams are central. Such teams collaborate by exchanging knowledge (product, process, service) and rights (patents, trade secrets, copyrights and trademarks). Exchange of knowledge is enabled and supported by advanced information management systems.

Knowledge exchange as required in TE processes is not free of risks. Risk may exist in terms of product piracy, plagiarism, counterfeits, theft of data, and cyber crime. The risks that actors encounter in a TE process depend on the type of interdependencies that they have. Three types of interdependencies have been described: pooled, sequential and reciprocal. In TE projects, actors are often interdependent in all three ways, making them vulnerable to multiple sources of risk.

Managing risks is challenging, not only because of the multiple sources of risks, but also because of the trade-offs that arise in choosing a method to deal with the risk. In addition, the type of interdependency influences the degree of adaptability to changing circumstances and the ability to measure the performance of other actors, thus influencing the predictability of risks.

Several technical solutions exist to manage risks in knowledge exchanges. These solutions are not sufficient. Different types of contracts exist that can be used to manage actors' exposure to risk. In essence, three ways of risk management can be distinguished: risk transferring, risk altering, and risk sharing.

The paper has addressed ways in which risk management in TE processes can be realized. However, more research is needed to study existing TE processes with the lens of risk management and interdependencies. A more refined definition of risk

management situations than presented in this paper is needed to study existing processes (see e.g., [3; 20]). From such studies, normative models may emerge that will help companies in TE processes to anticipate, manipulate, and minimize risk. In addition, technical solutions need to be embedded in encompassing measures to manage risks.

References

[1] P.M. Wognum, J.H. Trienekens, The system of concurrent engineering, in: *Concurrent Engineering in the 21st century. Foundations and Challenges,* J. Stjepandic, P.M. Wognum, W.J.C. Verhagen (Eds.), Springer, Heidelberg, 2015, pp. 21-50.

[2] J. Stjepandic, H. Liese, A. Trappey, Intellectual property protection, in: *Concurrent Engineering in the 21st century. Foundations and Challenges,* J. Stjepandic, P.M. Wognum, W.J.C. Verhagen (Eds.), Springer, Heidelberg, 2015, pp. 521-554.

[3] M. Wever, P.M. Wognum, J.H. Trienekens, S.W.F. Omta, Managing transaction risks in interdependent supply chains: an extended transaction cost economics perspective, *Journal on Chain and Network Science,* 12(3) (2012), pp. 243-260.

[4] O.E. Williamson, Transaction-cost economics: the governance of contractual relations, *Journal of Law and Economics,* 22(2) (1979), pp. 233-261.

[5] M. Sobolewski, Technology foundations, in: *Concurrent Engineering in the 21st century. Foundations and Challenges,* J. Stjepandic, P.M. Wognum, W.J.C. Verhagen (Eds.), Springer, Heidelberg, 2015, pp. 67-102.

[6] M. Jemala, Systemic insights into nanotechnology patenting in EU countries, *Int. J. of Agile Systems and Management*, Vol. 8, 2015, pp. 1–22.

[7] R.P. Cysne, D. Turchick, Intellectual property rights protection and endogenous economic growth revisited, *Journal of Economic Dynamics & Control*, Vol. 36, 2012, pp. 851–861.

[8] P.E. Chaudhry, Changing levels of intellectual property rights protection for global firms: A synopsis of recent U.S. and EU trade enforcement strategies, *Business Horizons*, Vol. 49, 2006, pp. 463-472.

[9] C.-J. Chen, T.-C. Liu, M.-A. Chu, Y.-C. Hsiao, Intellectual capital and new product development, *J. Eng. Technol. Manage.*, Vol. 33, 2014, pp. 154–173.

[10] F. Bernstein, A. Kök Gürhan, A. Meca, Cooperation in assembly systems: The role of knowledge sharing networks, *European Journal of Operational Research,* Vol. 240, 2015, pp. 160–171.

[11] O.E. Williamson, Outsourcing: transaction cost economics and supply chain management, *Journal of Supply Chain Management,* 44(2) (2008), pp. 5-16.

[12] J.D. Thompson, *Organization in action: social science bases of administrative theory,* McGraw-Hill, New York, NY, USA, 1967.

[13] G.A. Akerlof, The market for 'lemons': quality uncertainty and the market mechanism, *Quarterly Journal of Economics,* 84 (1970), pp. 488-500.

[14] K.J. Dooley, T. Yan, S. Mohan, M. Gopalakrishnan, Inventory management and the bullwhip effect during the 2007-2009 recession: evidence from the manufacturing sector, *Journal of Supply Chain Management,* 46(1) (2010), pp. 12-18.

[15] H.L. Lee, V. Padmanabhan, S. Whang, The bullwhip effect in supply chains, *Sloans Management Review,* 38(3) (1997), pp. 93-102.

[16] T.H. Chiles, J.F. McMackin, Integrating variable risk preferences, trust, and transaction cost economics, *The Academy of Management Review*, 21(1), pp. 73-99.

[17] J. Hallikas, I. Karvonen, U. Pulkkinen, V.-M. Virolainen, M. Tuominen, Risk management process in supplier networks, *International Journal of Production Economics,* 90 (2004), pp. 47-58.

[18] H.A. Simon, *Models of man: social and rational. Mathematic essays on rational human behavior in a social setting,* John Wiley & Sons, New York, NY, USA, 1957.

[19] A. Biahmou, J. Stjepandić, Towards Agile Enterprise Rights Management in Engineering Collaboration, *Int. J. of Agile Systems and Management*, Vol. 9, No. 4, 2016, in press.

[20] M. Wever, P.M. Wognum, J.H. Trienekens, S.W.F. Omta, Supply chain-wide consequences of transaction risks and their contractual solutions: towards an extended transaction costs economics framework, *Journal of Supply Chain Management*, 48(1) (2012), pp. 73-91.