A Taxonomy for Ensuring Institutional Compliance in Utility Computing

Tina Balke

University of Bayreuth,
Chair for Information Systems Management,
Universitätsstr. 30, 95447 Bayreuth, Germany
http://www.bwl7.uni-bayreuth.de/en/index.html

Abstract. With the ongoing evolution from closed to open distributed systems and the lifting of the assumption that agents acting in such a system do not pursue own goals and act in the best interest of the society, new problems arise. One of them is that compliance cannot be assumed necessarily and consequently trust issues arise. One way of tackling this problem is by regulating the behavior of the agents with the help of institutions. However for institutions to function effectively their compliance needs to be ensured. Using a utility computing scenario as sample application, this paper presents a general applicable taxonomy for ensuring compliance that can be consulted for analyzing, comparing and developing enforcement strategies and hopefully will stimulate research in this area.

Key words: Institutions, Compliance, Enforcement, Regimentation, Norms, Sanctions, Utility Computing

1 Self-Interested Agents in Utility Computing

1.1 The Vision of Utility Computing

The vision of Utility Computing (UtiC) has gained significant interest in the last years and has become a popular buzzword. The word "utility" is used to make an analogy to the provision of other services, such as electrical power, the telephone, gas or water, in which the service providers seek to meet fluctuating customer needs, and charge for the fungible resources they sell based on usage rather than on a flat-rate basis[1]. In the computing context examples of such resources are storage space, server capacity, bandwidth or computer processing time. UtiC envisions that in contrast to traditional models of web hosting where

[1] It is important to note that although the services offered by the service providers are individualized, their basic components are very standardized resources that can be easily exchanged. Thus, a telephone provider for example may provide his customers with very different telephone packages, however the underlying resources he uses are standardized telephone units.

Dagstuhl Seminar Proceedings 09121
Normative Multi-Agent Systems
http://drops.dagstuhl.de/opus/volltexte/2009/1901

the web site owner purchases or leases a single server or space on a shared server and is charged a fixed fee, the fixed costs are substituted by variable costs and he is charged upon how many of the fungible resources he actually uses on demand over a given period of time in order to perform his computationally intensive calculations. The business idea behind this vision is that if a company has to pay only for what it is using it can adapt its cost structure and will be able to economize, i.e. save money, while the company offering utility computing resources can benefit from economies of scale by using the same infrastructure to serve multiple clients [8].

Looking at the nature of the resources sold in the UtiC context as well as the potential number of transactions that might be conducted in such an infrastructure, it seems reasonable to argue that UtiC is an ideal field of application for automated negotiations using artificial agents [16]. Thus, the resources traded in UtiC have a high degree of standardization, and furthermore the open interaction system as well as the high number of repetitive transaction, suggest the usage of artificial agents that act on behalf of their human owners. Furthermore, as mentioned in the AgentLink Roadmap [25], Multi-Agent-Systems (MAS) offer strong models for representing complex and dynamic environment that cannot be analyzed mathematically any more, but need to be simulated. However when thinking in the lines of this vision, several problems occur, such as the question about the risks involved in UtiC transactions. Thus, it has to be ascertained that the bilateral economic exchange envisioned in UtiC is very likely to involve risks, such as risks resulting from strategic- and parametric uncertainties, that shall be explained in the next section with regard to the problem of self-interested agents [38].

For the further analysis it has to be noted that this paper views UtiC as one possible field of application of electronic institutions or e-commerce. Nevertheless as it is a good example of an open distributed market that can be simulated with MAS simulation, it is explained in more detail at this point and will be used as example in the course of the paper.

1.2 Strategic Uncertainties resulting from Self-Interested Agents

As noted at the end of the last section, two main kinds of uncertainties exist in UtiC transactions, namely strategic- and parametric uncertainties. Whereas the latter ones refer to environmental uncertainties that cannot (or only with a disproportionate effort) be reduced by the UtiC participants, the strategic uncertainties concern the question of whether the transaction partners are willing to comply with what has been agreed on or not; and whether, if a transaction has had an adverse outcome, this was due to bad luck or bad intentions [26, 21]. Thus, if a buyer does not receive the promised UtiC resources from the seller, it is often hard to judge whether the seller did not deliver intentionally, or whether the transaction failed, because the network broke down for example.

The basic assumption behind this the problem of strategic uncertainty thereby is that agents are rational believe forming utility maximizing entities. Thereby it is assumed that the agents do not necessarily always act in the best interest

of the societies global (or social) welfare. Instead they are likely to pursue their individual goals and try to maximize their profit (in terms of a maximization of their utility function) [31]. That is why agents may choose to not fulfill a contract as promised, if they expect a higher own utility from this. Thereby the decisions about the utility of different options by each agent are based on the limited information the particular agent has about the environment (i.e. the agents have a bounded rationality). As a result it becomes difficult to assess and control the utility functions of all participating agents. As a consequence it is very challenging from a UtiC environment designers point of view to control that the overall UtiC market outcome is as desired.

As a result institutions are needed that influence the utility functions of the agents and create incentives in such a way that cooperation is the dominant strategy and strategic uncertainty can be reduced to a minimum extent. In the next section the term institutions as used in this paper will be explained and the roles of institutions for regulating and controlling UtiC will be analyzed in more detail (2). Thereby special focus will be on the ensuring of the compliance with the institutions in UtiC as "if not being enforced effectively, [institutions] are nothing more than a decorative accessory" [9]. In the course of the analysis of the compliance-ensuring of institutions for UtiC, as the main contribution of this paper, in section 3 a taxonomy will be developed that tries to combine all elementary compliance-ensuring options in one table and to classify them in a expedient way. In a second step, the different elements of the taxonomy will be explained in detail in the sections 3.1–3.5 with the help of UtiC examples. Although, the main focus of this paper is UtiC, UtiC itself is just seen as a sample application for open distributed systems by the author. Thus, the author aims at presenting a general applicable taxonomy that can be consulted for analyzing, comparing and developing compliance-ensuring strategies and hopefully will stimulate research in this area. In a last step in this paper a research proposal will be made how to evaluate the taxonomy elements one against the other (chapter 4). Thereby 5 performance indicators will be presented that shall serve as a starting point for this analysis. Furthermore a research outline will of how the mechanisms shall be evaluated will be presented (chapter 4).

2 Ensuring Compliance of Institutions for Controlling Utility Computing

2.1 Institutions in Utility Computing

As mentioned in the last section, resulting from the openness of UtiC environments two problems arise: First of all anybody can participate in such an infrastructure and act intentionally and optimally towards their own specific goals (i.e utility functions). The second problem is that the overall social welfare of the system emerges as a result of the individual decisions and actions of the individual agents. However the utility functions that the agents base their decisions on are dynamic and normally private information of the individuals

and are therefore hardly predictable for the UtiC environment designers. As a result, "appropriate" mechanisms that foster compliance and regulate the UtiC environments (in terms of defining a regulative framework as well as sanctions for non-compliance with the framework[2]) need to be applied in order to achieve an "acceptable" overall behavior. The most promising mechanism, which will be addressed in this paper is the usage of institutions. Institutions alter the relative prices for defections and thereby create incentives for a system-conform behavior. This paper thereby understands the term institutions as often used in new institutional economics, namely is follows:

> **Institutions** are formal (e.g. statute law, common law, regulations) and informal structures (e.g. conventions, norms of behavior and self imposed codes of conduct) and mechanisms of social order and cooperation governing the behavior of a set of individuals by attributing rights and obligations to them. They are identified with a social purpose and permanence, transcending individual intentions, and with the making and compliance-ensuring of rules governing cooperative human behavior and thereby define the social outcomes that result from individual actions [29, 33].

Looking at this definition three main aspects can be remarked. The first one is that in the institutional economic view institutions are understood as a very abstract notion of a set of norms or social structure. Hence norms are seen to be component of institutions, which are the overall concept of a regulative framework. The second aspect to be remarked concerns the role of institutions, namely the setting up of a framework of rules and actions in which the agents have to operate. This framework not only defines what agents should and should not do, but erects sanctions to be applied if the framework is violated. And this is where the third main aspect comes into play: the compliance-ensuring component. As North phrased it in [28] with regard to ensuring compliance:

> "...[it] poses no problem when it is in the interests of the other party to live up to agreements. But without institutional constraints, self-interested behavior will foreclose complex exchange, because of the uncertainty that the other party will find it in his or her interest to live up to the agreement."

What North formulated in this statement is very straight forward: the compliance with an institutional framework poses no problem, if no self-interested behavior is involved. If however – as in UtiC – this is not the case and agents can exhibit self-interested behavior, it is important that institutions do not only state a set of rules, but it needs to be taken care that their compliance is ensured, because otherwise the strategic uncertainties arising might negatively influence the usage of an environment (e.g. UtiC).

[2] In this paper special focus will be on regulative rules as they pose problems in terms of compliance-ensuring. Although being of high importance as well constitutive rules will be omitted as their non-compliance leads to nullity [20].

After this brief description of the role of institutions and especially the ensuring of their compliance in UtiC, in the next section, the related work relevant for the implementation of institutions in open distributed environments such as UtiC shall be reviewed. Thereby special focus will be once again on the compliance-ensuring aspect as it is has a key function in the success of every institutional setting.

2.2 Related Work

Already in 1998, Conte et al. [10] pointed out two distinct sets of problems relevant for MAS research on norms: (1) the interaction of different autonomous agents on a norm-governed basis and (2) the interaction of individual autonomous agents with the norms (including the acquisition and the violation of norms). This problem definition has been expanded by Boella and van der Torre [4] to include a third question that deals with the evolution of norms. The first of the three questions has been discussed at length by researchers using game-theoretic approaches [4]; however a model integrating these approaches with the different social, cognitive and normative concepts is still missing. The second question has been studied by Broersen et al. [7] for example, who focused on the agent architecture for determining how agents can acquire and violate norms and how norms in turn influence agent behavior. Last but not least, the third question has been dealt with by Verhagen [37] and some economic commerce researchers. Verhagen distinguished between norms created by legislators, norms negotiated between agents and norms emerging spontaneously and thereby laid the groundwork for a number of papers about protocols and social mechanisms for the creation [5] and agent mediated evolution of norms [34] in MAS. In spite of this intensive research on the creation of norms in MAS, little work has been done explicitly addressing the ensuring of the compliance with such norms. Thus, although trust and reputation mechanisms as centralized (e.g. eBay) and decentralized coordination and compliance-ensuring instances [32] have been discussed by a number of researchers, the mechanisms tend to concentrate on specific use cases and often fail to address the importance of these mechanisms in the compliance context. Thus, in many papers it is explicitly assumed, that all normative regulations can be asserted and therefore little or no thought is given on what happens if this assumption cannot be fulfilled, although many scientists have stated that institutions and norms are more or less senseless if their compliance cannot be ensured [9].

One of the few papers that deals with compliance and analyzes at what levels it can be applied in a system was written by Vázquez-Salceda et al. [36], who not only make a distinction between regimentation and enforcement, but also elaborate on the levels of observability of norm violations. Other authors that address the compliance topic in their papers include D. Grossi [19, 20] who also distinguished between enforcement and regimentation, L. van der Torre, G. Boella and H. Verhagen (see [4] or [5] for example) as well as A. Perreau de Pinninck, C. Sierra and M. Schorlemmer [30], A. Artikis, M. Sergot and J. Pitt [1], M. Esteva, J. Padget and C. Sierra [15] or A. Garcia-Camino, P. Noriega

and J. A. Rodriguez-Aguilar [17]. All these papers elaborate on the importance of suitable mechanisms for ensuring compliance in distributed systems and propose mechanisms for specific scenarios. However in these papers, little analysis can be found, examining and comparing the different compliance ideas based on a common setting and researching on the interplay of the different concepts as well as their applicability for certain settings. That is why, this paper aims at providing a first step into the research just mentioned by presenting a comprehensive taxonomy for ensuring compliance with institutions, that can be used not only as a basis for analyzing different compliance mechanisms, but also for comparing, combining and in general developing corresponding strategies.

3 A Taxonomy for Ensuring Institutional Compliance in Utility Computing

After having had a brief look at the existing literature about institutions and the ensuring of their compliance in the last section, in this section a taxonomy of all methods through which compliance can be administered shall be developed. The goal of this endeavor is to illuminate the general concept of ensuring compliance as well as its different potential forms of implementation.Thereby, first of all, the cornerstones of the taxonomy (the column heads in figure 1) will be explained. This will be followed by a detailed analysis of the resulting compliance-ensuring mechanisms. The ideas for the taxonomy are based on works by Ellickson [13] (that were already cited by North [28] as theoretical "enforcement" foundation) and works by Grossi [19, 20] who made a distinction between regimentation and enforcement and proposed a basic classification mechanism for enforcement concepts.

To start, as already defined in section 2.1, an institutionally tailored system consists of a framework of *rules* defining normatively appropriate behavior. The compliance with these rules is ensured through (positive or negative) *sanctions*, the administration of which is itself governed by rules. Concerning the sanctions, institutionally entailored systems typically employ both rewards and punishment – both carrots and sticks – to influence behavior. In order to administer these positive and negative sanctions, agent behavior is usually divided into three categories [13]:

1. good behavior that is to be rewarded,
2. ordinary behavior that warrants no response (as giving a response to the most common behavior only tends to increase the costs of administering sanctions) and therefore will not be discussed any further in this paper, and
3. negative behavior that is to be punished.

However, before any compliance-ensuring can take place another aspect has to be thought about: the behavior of the agents needs to be monitored in order to categorize it and apply the right kind of sanction[3]. This monitoring can

[3] In the further course of this paper, the main focus will be on sanctions that punish negative behavior, as these are especially relevant in the context of strategic uncer-

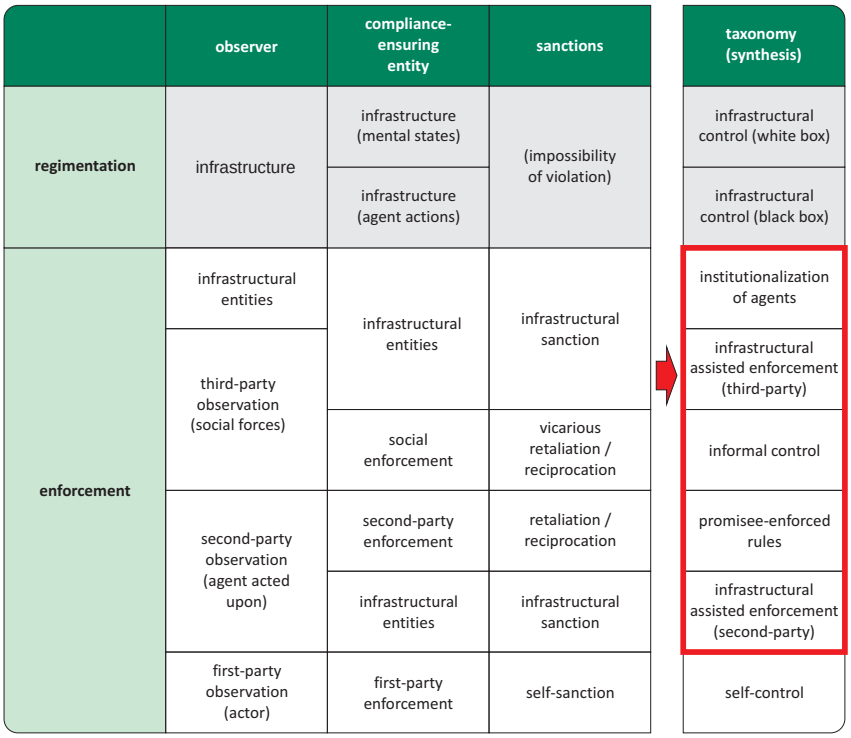

Fig. 1. Taxonomy for Ensuring Institutional Compliance

be done by *observers* in a system. Thereby it seems useful to distinguish between 4 types of observers, that not only monitor the behavior of the individual agents, but can act as information source for both rules of behavior and sanctions: a first-party observer who controls his accordance with the rules in a system (whether self-imposed or imposed by other sources) himself, a second-party observer who observes the behavior of his transaction partner(s), third-party observers that control the behavior of other agents the system and last but not least the infrastructure (in the sense of both, the infrastructure as a whole as well as infrastructural entities) as observer. Once, the behavior of the agents is observed, the ensuring of compliance can take place. This can either be done by te observer of the violation or by another party. In total this paper distinguishes 4 different kinds of *compliance-ensuring entities* which all have different kinds of sanctions that can be used for ensuring institutional compliance. The 4 enforcers are: the infrastructure provided by the UtiC designer (including institutional entities as a sub-group), social groups (up to the society as whole) consisting of non-infrastructural entities, second-party enforcers (i.e. the transaction partners) and first party-enforcers.

As a result of these considerations, the *taxonomy* that can be seen in the final column of figure 1 can be developed. The taxonomy is the synthesis of the 4 types of observers that can spot the behavior of agents with regard to the institutional framework (e.g. violations or actions in accordance with the institutions) and the 4 types of compliance ensurers that (depending on their type) can apply sanctions (in order to ensure compliance). It consists of 8 different kinds of combined systems that represent all compliance-ensuring concepts that can be applied reasonably: *infrastructural control (white box)*, *infrastructural control (black box)*, *institutionalization of other agents*, *infrastructural assisted enforcement (third-party)*, *promisee-enforced rules*, *infrastructural assisted enforcement (second-party)* and *self-control*.

3.1 Regimentation vs. Enforcement

After briefly explaining the main categories (i.e. the column heads in figure 1), as a last step before going into detail about the synthesized taxonomy, the distinction between the two row heads of figure 1, i.e. *regimentation* and *enforcement* shall be explained.

Regimentation refers to the ensuring of institutional compliance by making violation states unreachable via an appropriate infrastructure (i.e. allowing for no deviation from institutionally defined behavior) so that no compliance issues occur [23]. This is normally done in either of the following two ways.

1. By ensuring that all agents' mental states are accessible to the system (closed systems), and can be altered to be in accordance with the normative framework. Thus, agents are treated as a white box that's content can be by

tainties. However all the taxonomy elements of this paper can be thought of in form of reward mechanisms for good behavior as well.

analyzed and altered (this concept is for example applied in the KAoS architecture [6]). In the taxonomy this idea is referred to as *infrastructural control (white box)*.

2. In case the mental states are not accessible to the system (i.e. the inner states of an agent are a black box to the system), compliance is ensured by constraining the actions of the individual agents. This idea is for example used in systems such as ISLANDER that uses so-called "governors". In ISLANDER agents do not act directly but through their governor, who can consequently check all actions. Hence, if an agent wants to send a message that is not allowed, the governor will not send it and consequently institutional compliance is ensured [14]. In the taxonomy this idea is referred to as *infrastructural control (black box)*.

In contrast to regimentation where non-compliance is made impossible by controlling everything that might lead to a violation of the institutional framework, enforcement "only" uses indirect mechanisms in order to ensure compliance. Thus in enforcement positive or negative incentives are being used that shall render compliance the preferable choice for an agent.

Putting it simple: regimentation pursues the idea of 100 per cent control (of either agent actions or their mental states) and consequently compliance can be always be ensured, however it limits the autonomy of the agents. Furthermore it seems difficult to implement it in open distributed settings such as UtiC and might become inoperative in case agents have agreed to conduct the actual transaction outside the monitored environment (of course messages of such type could be filtered by the system, this aspect is neglected at this point). Looking at eBay for example, although the transaction partners agree to live up to their agreements in a transaction (e.g. deliver a good after the money has been set), eBay cannot force them to do so, because the physical transaction takes place outside the eBay marketplace and thus at that point eBay has no direct control over either the mental states or the actions of the individuals acting on eBay. Last but not least one further possible problem arises with regimentation, a problem with its costs. The term costs thereby is not necessarily understood in monetary terms, but can for example be seen in the increased number of messages (infrastructural resources) that are needed for the 100 per cent monitoring. This is where enforcement steps in. Although maybe preferable in some situations, enforcement aims at as much control as possible control at resonable costs for the compliance. As already mentioned it instead makes use of negative and positive incentives that can be applied not only by the organization, but all agents acting in the system as well and therefore can reduce the costs of UtiC designers, by reducing their monitoring work.

Now that the heads of the table columns have been discussed, finally the combined systems that result from the intersection of the components of compliance-ensuring shall be explained in more detail. These are infrastructural control (white / black box), the institutionalization of other agents, infrastructural assisted enforcement (third-party / second-party), informal control, promisee-enforced rules and self control. Thereby special focus will be on the enforcement

related concepts and infrastructural control (i.e. regimentation) will be neglected as it has just been discussed.

3.2 Institutionalization of Agents

The institutionalization of other agents can be thought of in form of the implementation of agents with special rights (i.e. some kind of police agents) that patrol the environment (in our example the UtiC environment) and sanction negative behavior (i.e. non-compliance) if spotted. These police agents are given their special rights by the UtiC designer (i.e. they are infrastructural entities and receive their power from the institutional framework provided by the UtiC infrastructure) and consequently perform an institutional compliance-ensuring. However in contrast to regimentation the police agents do not control all actions but only act as enforcers if violations are spotted. The spotting of the institution-violation is done by the police agents themselves who test the behavior of agents at random and react to what they detect. Looking at the kind of sanctions that can be applied by the police agents several sanctions can be thought of (depending on the severity of the non-compliance) such as a complete exclusion of the UtiC system to penalty payments or replacement deliveries of the resources (e.g. disk space).

3.3 Infrastructural Assisted Enforcement (Second-Party / Third-Party)

The concepts of infrastructural assisted enforcement are very close to the idea of the institutionalization of other agents. Thus again infrastructural entities act as compliance ensuring entities that can make use of sanctions ranging from a complete exclusion of the UtiC system to penalty payments or replacement deliveries of the resources (e.g. disk space). However in contrast to the concept of the institutionalization of other agents, not the infrastructural entities act as observers, but either the agent that was acted upon, i.e. the agents that was deceived by its transaction partner (second-party observer) or the observation is done by a third-party, i.e. an agent that is not involved in the transaction but has spotted the non-compliance of one actor. These observers then call the infrastructural entities for conducting the sanctioning in order to assure compliance. Thus, in contrast to the institutionalization of other agents where the infrastructural entities act on their own observations, in these two cases, an additional communication effort must be made that bears two problems. First of all the additional communication needed might result in a longer reaction time and furthermore, the infrastructural entities need to verify the testimonies made to them as the agents my lie on purpose in order to have rival agents sanctioned (and thereby profit themselves).

One sample application of this taxonomy element (with second-party observers) was described by Balke and Eymann [2, 3] that seized an idea by Güth and Ockenfels [22] and analyzed the effects of an arbitration board as infrastructural entity that can be called by any agent that has been deceived. Using

an game-theoretic approach, in their paper they showed that with the help of the arbitration board, it is possible to increase trust and reduce strategic uncertainty in open environments such as UtiC markets where software agents trade standardized resources on behalf of their human owners, even if the arbitration board is not equipped with superior detection capabilities, but uses Bayesian rules for assessing the trustworthiness of the agents.

3.4 Informal Control and Promisee-Enforced Rules

Two other concepts that can be thought of where second- or third party observer information is being used are informal control and promisee-enforced rules. Although looking different in figure 1 at the first glance (i.e. in promisee-enforced rules concept it is the agent that has been promised something (i.e. he is a promisee) but didn't receive it as promised who observes and sanctions the non-compliance, whereas in the informal control concept third-party agents observe and sanction) the two concepts are closely interrelated and are therefore presented together in this section. This interrelation can be understood best when thinking about examples for the two concepts. Thus promisee-enforced rules can be found in image-based trust mechanisms, whereas informal control can be found in reputation mechanisms.

Image is a global or averaged evaluation of a given target on the part of an individual. It consists of a set of evaluative beliefs [27] about the characteristics of a target. These evaluative beliefs concern the ability or possibility for the target to fulfill one or more of the evaluator's goals, e.g. to behave responsibly in an economic transaction. An image, basically, tells whether the target is "good" or "bad", or "not so bad" etc. with respect to a norm, a standard, a skill etc.

In contrast *reputation* is the process and the effect of transmission of a target image. The evaluation circulating as social reputation may concern a subset of the target's characteristics, e.g. its willingness to comply with socially accepted norms and customs [11].

Putting it simple, an image is the picture an individual has gained about someone else (the target) based on his own previous observations of that target. If using reputation, the individual expands the information source about the target beyond its own scope and includes the information of others about the target as well [24].

Applying this to the taxonomy example the following picture can be drawn: in the promisee-enforced rules concept, it is the promisee who acquires an image of the agent it is interacting with. In case the other agent does not perform as promised that promisee can sanction the non-compliance by for example not interacting with the agent once more, etc. In contrast in case of informal control, third-party agents observe a transaction and form an own image about the transaction participant. Then the individual images of agents are shared between the agents and hence they are aggregated by the society (e.g. with the help of gossip) and agents that did not comply with the institutional framework have to fear that every agent that receives the information about their non-compliance

will not act with them in the future, thus in this example the whole society functions as enforcers.

3.5 Self-Control

The last part of the taxonomy that shall be discussed in this paper is self-control. In contrast to all other compliance-ensuring mechanisms presented so far, it does not included any additional party, but only the agent performing an action itself. This agent is assumed to have an own normative value system that it was given by its principal and constantly checks whether his actions are in accordance with that own value system and the institutional framework of the UtiC environment (i.e. the agent is its own observer). Thereby it has to be noted that the two normative value systems (i.e. the private one of the agent and the UtiC one) can contradict and needn't necessarily be consistent with one another. Based on the normative value system the agent can then decide to sanction itself. An example of such a self-control scenario in UtiC could be that an vendor of UtiC resources that didn't deliver what he promised (e.g. he promised 1 Tera byte of hard disk space available, but only could provide 0.99 Tera byte) is discontent with his performance (although the buyer might not have complained) and as a result offers his buyer a refund for the money paid.

4 Further Research

After presenting this short taxonomy for compliance-ensuring mechanisms in a next step the highlighted enforcement mechanisms shall be evaluated one against the other. Thus, the different enforcement mechanisms will be evaluated against performance indicators derived from literature. These performance indicators can be sen in figure 2.

With the help of the taxonomy developed that aims to prototypically represent existing enforcement mechanisms, an analysis of the technological restrictions of UtiC as well as economic theory, finally a sample UtiC market model without and with the corresponding enforcement mechanisms will be deduced as a next step. This market model will serve as the initial point for the later simulations.

The simulation will be conducted in form of a MAS simulation because MAS offer strong models for representing complex and dynamic environment such as UtiC markets that cannot be analyzed mathematically any more, but need to be simulated. For the simulation a social science simulation research process that is based on works of Gilbert and Troitzsch [18] and Dooley [12] and can be seen in figure 3 will be used.

Looking at the process, first of all an abstract model has to be conceptualized and designed that represents the described UtiC market (with and without the different enforcement mechanisms that are derived from the compliance-ensuring taxonomy) adequately. This includes the consideration of the specification of UtiC. For these UtiC specifications, specifications from existing computational

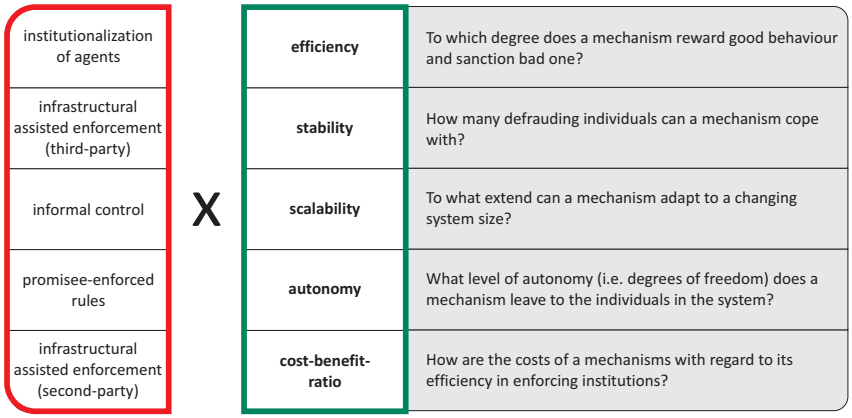

Fig. 2. Performance Indications vs. Mechanisms

Grid and systems such as the LHC Grid, TeraGrid and GEON-Grid or Grid5000 [35] will be used, as these are existing technical implementations of the economic vision of UtiC.

Once the model has been designed, the building issue needs to be considered, i.e. the model just designed has to be implemented in a MAS simulation environment. Therefore the SimIS simulation environment that is based on the Repast Simphony Simulation Toolkit will be used as it allows to model computational Grid systems in form of "physical" nodes and edges between these nodes, whereas each nodes hosts different agents, which fulfill a certain role each. Afterwards, the next step in the simulation research process is to check if the current model is actually doing what it is expected to do. This process of checking is called verification. In addition to this step the simulation has to be ensured to reflect the behavior of the target, which is called validation. "Validity can be ascertained by comparing the output of the simulation with data collected from the target." [18]

The idea of the simulation experiment is that in the initial form of the simulation, the market model will be implemented in the simulation environment without an enforcement mechanism and will be calibrated in the course of the simulations. Thus, throughout the simulation the UtiC market setting will be altered in terms of the enforcement mechanism applied. In the analysis of the simulation results afterwards, the initial form of the market as well as the market outcome depending on the enforcement mechanism will serve as a reference for the efficiency of different enforcement concepts with regard to the UtiC market setting.

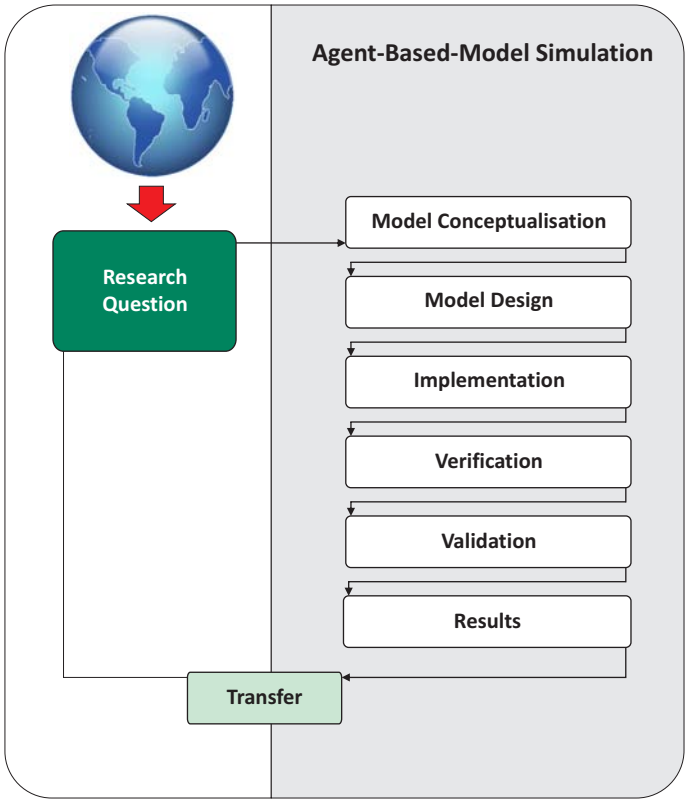

Fig. 3. Simulation Process

After the test of the hypotheses and the corresponding calibration of the simulation, the simulation results will be analyzed and evaluated in order to arrive at set-up specific simulation results in a first step, as well as generalize-able results for the UtiC domain in a second step. Resulting from these evaluations in a last step a generalization is aimed at analyzing which enforcement mechanisms works best for UtiC in which situation.

5 Conclusion

Using an UtiC example, in this paper a taxonomy for ensuring-compliance in open distributed systems was presented. The taxonomy that was synthesized based on considerations of the components and participants of compliance ensuring mechanism in general (see section 3) consists of 8 idealized concepts that were discussed with the help of examples in the further course of the paper. The author views these concepts as a basis for not only analyzing different compliance mechanisms, but also for comparing, combining and in general developing corresponding strategies. Thus in the future work the author plan to simulate prototypical implementations of the taxonomy elements (all based on the same simulation setting) and analyze the performance with regard to compliance ensuring and especially the corresponding cost-benefit ratio. Furthermore, a detailed analysis of the interplay of the taxonomy elements will be made, as in theory not only the individual taxonomy elements are realistic for compliance ensuring strategies, but any combination of the elements is thinkable. However in order to derive at this point, first of all the very high-level concepts presented in this paper need to be made "processable". That means that first off all, in the next step the concepts will be analyzed with regard to their transferability to a logical sound and operational Agent-Based Model. This model will then be used as described in chapter 4. This means that an Agent-Based Model as "processable" model of the economic theory will be developed that will that serve as starting point for a MAS simulation. This simulation aims at evaluating the enforcement concepts that were presented in this paper with regard to the performance indicators mentioned before. With the help of the results the authors hope to be able to draw more general conclusions and arrive at propositions which enforcement concept seem appropriate if only certain performance indicators need to be fulfilled.

References

1. A. Artikis, J. Pitt, and M. Sergot. Animated specifications of computational societies. In *AAMAS '02: Proceedings of the first international joint conference on Autonomous agents and multiagent systems*, pages 1053–1061, New York, NY, USA, 2002. ACM.
2. T. Balke. An extended "court game" - using institutions to foster compliance in open multi-agent systems. In *Proceedings of the Sixth European Workshop on Multi-Agent Systems (EUMAS 2008)*, 2008.

3. T. Balke and T. Eymann. Using institutions to bridge the trust-gap in utility computing markets - an extended "trust game". In *Proceedings of the 9. Internationale Tagung Wirtschaftsinformatik*, 2009.
4. G. Boella and L. van der Torre. A game-theoretic approach to normative multiagent systems. In *Dagstuhl Seminar Proceedings (Dagestuhl Seminar, 18.03. - 23.03.2007)*, Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2007.
5. G. Boella and L. van der Torre. Substantive and procedural norms in normative multiagent systems. *Journal of Applied Logic*, 6(2):152–171, 2008.
6. J. M. Bradshaw, S. Dutfield, B. Carpenter, R. Jeffers, and T. Robinson. Kaos: A generic agent architecture for aerospace applications. In *Proceedings of the CIKM '95 Workshop on Intelligent Information Agents*, 1995.
7. J. Broersen, M. Dastani, J. Hulstijn, and L. van der Torre. Goal generation in the boid architecture. *Cognitive Science Quarterly*, 2(3-4):428–447, 2002.
8. N. G. Carr. *Does IT matter?* Harvard Business School Press, Boston, MA, 2003.
9. J. S. Coleman. *Foundations of Social Theory*. Harvard University Press, Cambridge, MA, 1990.
10. R. Conte, C. Castelfranchi, and F. Dignum. Autonomous norm-acceptance. In *Intelligent Agents V (ATAL'98)*, volume 155 of *Lecture Notes on Computer Science*, pages 99–112. Springer, Berlin, Germany, 1999.
11. R. Conte and M. Paolucci. *Reputation in Artificial Societies: Social Beliefs for Social Order*. Springer, October 2002.
12. K. Dooley. Simulation research method. In J. Baum, editor, *Companion to Organizations*, pages 829–848. Blackwell, London, 1990.
13. R. C. Ellickson. *Order without Law: How Neighbors Settle Disputes*. Harvard University Press, June 2005.
14. M. Esteva, D. de la Cruz, and C. Sierra. Islander: an electronic institutions editor. In *AAMAS '02: Proceedings of the first international joint conference on Autonomous agents and multiagent systems*, pages 1045–1052, New York, NY, USA, 2002. ACM.
15. M. Esteva, J. A. Padget, and C. Sierra. Formalizing a language for institutions and norms. In *ATAL '01: Revised Papers from the 8th International Workshop on Intelligent Agents VIII*, pages 348–366, London, UK, 2002. Springer-Verlag.
16. I. Foster, N. R. Jennings, and C. Kesselman. Brain meets brawn: Why grid and agents need each other. In *Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems, 2004. AAMAS 2004*, pages 8–15, 2004.
17. A. Garcia-Camino, P. Noriega, and J. A. Rodriguez-Aguilar. Implementing norms in electronic institutions. In *AAMAS '05: Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, pages 667–673, New York, NY, USA, 2005. ACM.
18. N. Gilbert and K. Troitzsch. *Simulation for the Social Scientist*. Open University Press, 2005.
19. D. Grossi. *Designing invisible handcuffs. Formal investigations in institutions and organizations for multi-agent systems*. PhD thesis, Utrecht University, 2007.
20. D. Grossi, H. M. Aldewereld, and F. Dignum. Ubi lex, ibi poena: Designing norm enforcement in e-institutions. In P. Noriega, J. Vázquez-Salceda, G. Boella, O. Boissier, M. Dignum, N. Fornara, and E. Matson, editors, *Coordination, Organizations, Institutions, and Norms in Agent Systems II*, pages 101–114. Springer, 2007.

21. W. Güth and H. Kliemt. Evolutionarily stable co-operative commitments. *Theory and Decision*, 49:197–221, November 2000.
22. W. Güth and A. Ockenfels. The coevolution of morality and legal institutions – an indirect evolutionary approach. *Journal of Institutional Economics*, 1(02):155–174, December 2005.
23. A. J. I. Jones and M. Sergot. On the characterization of law and computer systems: the normative systems perspective. In *Deontic logic in computer science: normative system specification*, pages 275–307. John Wiley and Sons Ltd., Chichester, UK, 1993.
24. S. König, T. Balke, W. Quattrociocchi, M. Paolucci, and T. Eymann. On the effects of reputation in the internet of services. In *Proceedings of the 1st Int. Conference on Reputation (ICORE 2009)*, 2009.
25. M. Luck, P. McBurney, O. Shehory, and S. Willmott. *Agent Technology: Computing as Interaction (A Roadmap for Agent Based Computing)*. AgentLink, 2005.
26. J. Martiensen. *Institutionenökonomik*. Verlag Vahlen, 2000.
27. M. Miceli and C. Castelfranchi. The role of evaluation in cognition and social interaction. In K. Dautenhahn, editor, *Human cognition and social agent technology*. Benjamins, Amsterdam, 2000.
28. D. C. North. *Institutions, Institutional Change and Economic Performance (Political Economy of Institutions and Decisions)*. Cambridge University Press, October 1990.
29. D. C. North. Institutions matter. Economics history working paper, 1994.
30. A. Perreau de Pinninck, C. Sierra, and M. Schorlemmer. Friends no more: norm enforcement in multiagent systems. In E. H. Durfee and M. Yokoo, editors, *AAMAS '07: Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems*, pages 640–642, New York, NY, USA, 2007. ACM.
31. L. Rasmusson and S. Janson. Agents, self-interest and electronic markets. *The Knowledge Engineering Review*, 14(2):143–150, 1999.
32. J. Sabater. *Trust and reputation for agent societies*. PhD thesis, Institut d'Investigació en Intelligència Artificial, Universitat Autonòma de Barcelona, 2003.
33. A. Schotter. The evolution of rules. In R. N. Langlois, editor, *Economic as process*, pages 117–133. Cambridge University Press, Cambridge, 1986.
34. C. Sierra and P. Noriega. Agent-mediated interaction. from auctions to negotiation and argumentation. In *Selected papers from the UKMAS Workshop on Foundations and Applications of Multi-Agent Systems*, pages 27–48, 2002.
35. W. Streitberger. *Einsatz von Risikomanagement bei der Steuerung von Grid-Systemen - Ein Analyse von Versicherungen anhand einer simulierten Grid-Ökonomie*. PhD thesis, University of Bayreuth, 2009.
36. J. Vázquez-Salceda, H. Aldewereld, and F. Dignum. Implementing norms in multiagent systems. In *Multiagent System Technologies*, volume 3187 of *LNAI*, pages 313–327. Springer, 2004.
37. H. Verhagen. *Norm Autonomous Agents*. PhD thesis, Stockholm University, 2000.
38. S. Voigt. *Institutionenökonomie*. Neue Ökonomische Bibliothek. UBT Verlag, 2002.