Noname manuscript No.
(will be inserted by the editor)

Ethical Requirements for Reconfigurable Technology

Francien Dechesne · Martijn Warnier · Jeroen van den Hoven

Received: date / Accepted: date

Abstract With the increasing use of information technology for different societal goals, the demand for flexible usage of appliances has risen. Making technology reconfigurable to keep it open to functionalities not yet determined in the design phase, could be a way of achieving this. This article is written against the background of a large scale research project developing reconfigurable sensors in order to achieve a continuous and affordable infrastructure for both safety and security (STARS). Our role in the project is to explore the ethical challenges the aspect of reconfigurability raises for sociotechnical systems such as sensor networks. In this short paper, we present an initial exploration of how such reconfigurability challenges the usual specification and assessment of functional and non-functional requirements. Such technology specifically requires an analysis of the composition and interaction of different contexts, and its translation into policies, which forms a challenge for the 'design for values' approach.

Keywords reconfigurability · sensor networks · security · design for values · context · policy design

The research presented in this paper is part of research project *Sensor Technology Applied in Reconfigurable systems for Sustainable security*: STARS [STA(2010)].

F. Dechesne
Philosophy
E-mail: f.dechesne@tudelft.nl

M. Warnier
Systems Engineering
E-mail: m.e.warnier@tudelft.nl

M.J. van den Hoven
Philosophy
E-mail: m.j.vandenhoven@tudelft.nl

Dept. of Technology, Policy and Management, TU Delft,
Jaffalaan 5, 2628 BX Delft, NL

1 Introduction: the STARS project

Our current society shows an increasing complexity and associated risks, under the influence of developments like globalization and the growing use and dependence on technology. In response to this, more technology is developed and deployed in order to manage both complexity and risks. Sensors (such as, e.g., cameras or motion detectors) are viewed as important sources of information that can be used to protect our society against threats on the one hand, and to help resolve crisis situations on the other. Such sensors are connected in networks, allowing for gathering and analyzing the combined information, and making it accessible to human decision makers.

The application area of security and safety have especially pushed the development of all kinds of sensor technology. It also motivated a large scale, 4.5 year research project in The Netherlands called STARS: Sensor Technology Applied in Reconfigurable systems for Sustainable security [STA(2010)]. The STARS project involves both academic and private research partners. The goal of the STARS-project is the development of "necessary knowledge and technology to be able to build reconfigurable sensors and sensor networks". By making sensors reconfigurable, the project aims to deliver a continuous and affordable infrastructure for societal security, but it also anticipates possible use in other application areas. Reconfigurable parts of sensor networks that will be looked at are antennas, receivers, transmitters, on-chip and off-chip communication. As an example, one may want to be able to transform a sensor network installed in a harbor for security purposes, e.g. to prevent theft or sabotage, into an information system for rescue workers during a fire in the same harbor.

The security domain is characterized by the great diversity of threats and the absence of warning time. The creativity of the opponent ensures that the circumstances change continuously and unpredictably so. It is therefore essential to be able to anticipate and respond adequately to new situations. The societal problem is that it takes too long, and it is too expensive, to invest over and over again in new systems to be developed to protect against ever changing threats. Truly successful security technologies should therefore satisfy a number of characteristics: reliable and affordable, sustainable and effective, multi-domain and multi-service. In the STARS-project, reconfigurable sensors are developed to have these characteristics. They allow for flexible application, because the functionality enclosed in the system should be relatively easy and quickly to adapt. In the expected deployment scenarios, reconfigurability is used to instantaneously optimize for foreseen situations and the corresponding tasks. In new -unexpected- scenarios reconfigurability is used to respond to circumstances that were unforeseeable at the time of the system development, by adapting the functionality of the system to the new situation.

With this as motivation, the feature of reconfigurability will be leading in the design and development of the architecture and technologies in the STARS-project. Although the first use cases primarily speak of police, fire brigade , security- and information services as intended users, it is expected that the technology, if successful, will cover a broader application area by a broader range of users. During the project, system concepts and application potential are to be defined and explored.

Reconfigurable sensor networks are developed to serve the societal goals of safety and security, but it is not just the technical features of the network that will determine the effect of the technology. The effect will be determined by the way in which the system with its features is embedded in social and societal structures: What data will be gathered and by whom? Who will handle the data? How will the data be used? Who determines the priority of functionalities, if the system is intended to serve different goals? The aspect of reconfigurability makes these questions even more complex, but also more pressing.

We illustrate these issues in the next section, where we describe a use case from the STARS project. The role within STARS of the authors of the current paper, is to evaluate societal and moral implications of the technology that is developed within the project. As the project in itself is still in its initial phase, this paper presents an initial exploration of questions we think will be the relevant ones, rather than giving theories and answers. In the rest of the paper, we aim to show that reconfigurable technology adds an extra challenge to design for values, because it pushes the specification of the intended functionality and use forward to after the design phase. The wide applicability of the technology in society (*logical malleability* in Jim Moor's terminology [Moor(1992)]) requires that societal and moral values are considered in the application phase, but ideally already in the design phase. With the flexibility of reconfigurable technology, this requires new tools, for instance in order to keep track of different and evolving contexts of use. In particular, the design of good usage policies becomes crucial.

2 Use Case: Sensor Usage in a Large Port Area

The intended application of the reconfigurable sensors and sensor networks is the safety and security domain. A use case for the sensor networks is for example the situation at a large port area (for example, the port of Rotterdam or Shanghai). Radar systems are used in large ports to monitor the movement of ships. Ship sizes can also be determined by these systems. Such radar systems consist of a number of radar devices, which send their collected data to a central control center. Here the data is processed to provide a full overview of the whole area. Other sensor data, for example from camera surveillance systems (CCTV: closed circuit television) or motion detectors (around security gates) are also sent here, providing even more information in case of an incident.

Numerous issues around safety and security can arise in a port environment, including fire hazards, drug trafficking, terrorism, people trafficking or transport of hazardous chemicals. During an incident all sensor data can be combined to coordinate emergency services. Reconfigurable sensors could be especially useful in such environments, since they are intended to be usable for different tasks as the need arises, whereas previously multiple sensor systems were required. Consider, for example, the case where a small plane crashes into the port area. The police might be worried that this is part of an organized terrorist attack, in which case (part of) the radar system can be reconfigured to look for other (low flying) planes. Information provided by the reconfigured radar system can be crucial for the police (and other services) to gain control of the situation.

However, the reconfigurability of the sensors also introduces a number of potential problems. First of all, by reconfiguring the radar system, the 'normal' radar view of the ships in the harbor is compromised: the spatial resolution will go down, making it harder to distinguish different ship sizes. Part of the harbor may not be visible at all. This might be acceptable in a crisis situation, but it does lead to another issue: Who decides if the radar system may be reconfigured, and under which circumstances? Is the fire brigade in charge or the police? Or perhaps the port authorities or the government? Clear policies need to be defined for this, policies that can become more complex as the sensor systems' reconfigurable functionality increases. Even if the aim is to make the technology almost instantaneously reconfigurable, it is still likely that there will be some processing time needed for each reconfiguration. This can be crucial in crisis situations:

during reconfiguration sensors cannot be used, leaving the control center in essence blind to the current situation. This may be acceptable if reconfiguration time is in the range of fractions of seconds, but longer delays may compromise the functionality of the technology.

Such issues stem from the same core problem: reconfigurable systems may provide multiple functionality and be flexible in extending functionality, but they cannot use the functionalities concurrently. One can either search for ships or for low flying planes, not both (at the same time). This adds to the already difficult task of balancing and prioritizing values, especially if different values are supported by different functionalities. Who gets to decide which value should be given priority in such situations?

3 What is reconfigurable technology?

Before we head on to discuss ethical and societal issues that we expect to come up in the development of reconfigurable sensor technology, we briefly reflect on the notion of 'reconfigurable technology'. It is useful to analyze the relationship between (re)configuration and (flexible) functionality of the technology.

Literally 'reconfiguration' means: to modify the configuration, i.e. the arrangement of the parts (of a system). Implicitly, at least within the STARS-project, it is taken that new configurations will lead to new functionalities and usages, in particular: functionalities that may not yet have been specified when the technology was developed. Hence, reconfigurability should serve to provide a flexibility in functionality beyond the design phase. Because the term 'functionality' often bears the connotation of being the particular use *for which something is designed*, it is probably better to use Gibson's terminology of *affordance* [Gibson(1986)]. Affordances of a technology can be defined as the action possibilities latent in the technology, and need not be designed-in intentionally. This is clearly demonstrated in the *dual use*-problem: technologies designed for peaceful purposes, such as the improvement of human health by biotechnology, can potentially also be used for harmful aims.

We would like to point out that configuration and functionality or affordance by no means have a one-to-one relationship. A piece of technology can have different affordances without having to be reconfigured, or even having to be reconfigurable. A simple stone can be a missile, but also a "paper weight, a bookend, a hammer, or a pendulum bob" [Gibson(1986), p.134]. Another painful example of this is how a car can be both a means of transportation, and a deadly weapon if intentionally used to drive into a group of people. Conversely, of course, not every reconfiguration -in the sense of: rearrangement of parts- will necessarily lead to new affordances of the technology.

Another question is what exactly counts as "reconfiguration", and what goes beyond by adding parts. It is current practice nowadays to extend the affordances of sensor systems by processing the signals using computers. Think for example of the enhancement of CCTV systems with software that processes faces and compares these to a database with known subjects [Zhao et al(2003)] in order to identify them. In a sense this extension could be described as a reconfiguration of the CCTV system, since the original functionality of the system is altered for a specific purpose. But we take it that not every alteration or extension of *functionality* necessarily counts as a *reconfiguration*. When adding computers for information processing in a sensor network, this is more than a rearrangement of existing parts. We would call this combining technologies rather than reconfiguring the sensor system.

Returning to the concrete background of this paper: what kind of reconfigurability can we expect within the STARS-project? The ultimate goal of the project is to develop sensors and sensor networks with as much (potential) functionality as possible. The project proposes to achieve this by making the hardware reconfigurable, which involves mainly analogous front-ends (infrared, radar, etc.) and digital signal processing. We think the resulting range of possible reconfigurations will be rather limited, but as such, this will provide an interesting starting point. The system concepts and architecture have yet to be developed. Even so, methodological questions are already raised by making parts of the architecture reconfigurable, such as those concerning testing procedures, software-hardware partitioning and composability (as pointed out for reconfigurability in the context of software architecture in [Guo(2006)]).

On a high level, one could even state that STARS aims to create the *affordance* to address future, yet unknown, applications by making the technology reconfigurable. In our involvement in the STARS-project, we aim to identify specific ethical challenges related to the reconfigurability of technology, although we will also touch upon more general issues of multiple and flexible functionality, with the goal of creating awareness and anticipating these challenges in the research and development phase of the technology. In this process, we will address the question whether design for values for reconfigurability related values asks for a different approach, and how design for values for reconfigurable technology relates to proposed approaches to the ethics of emerging technologies (such as, for example, Ethical Technology Assessment [Palm and Hansson(2006)] or Anticipatory Technology Ethics [Brey(2011)]).

4 Reconfigurability as a challenge for design for values

When looking for ethical challenges raised by the feature of reconfigurability, it is natural to turn to ethical theories for what seems the ultimate reconfigurable technology: the 'universal machine', i.e. the computer. In his seminal paper "What is Computer Ethics?" [Moor(1992)], James Moor refers to the *logical malleability* of computers as the essence of the revolutionary character of computer technology, from which the need for a separate attention for computer ethics follows:

> "The essence of the Computer Revolution is found in the nature of a computer itself. What is revolutionary about computers is logical malleability. Computers are logically malleable in that they can be shaped and molded to do any activity that can be characterized in terms of inputs, outputs, and connecting logical operations. [...] This is all I need to support my argument for the practical importance of computer ethics. In brief, the argument is as follows: The revolutionary feature of computers is their logical malleability. Logical malleability assures the enormous application of computer technology. This will bring about the Computer Revolution. During the Computer Revolution many of our human activities and social institutions will be transformed. These transformations will leave us with policy and conceptual vacuums about how to use computer technology. Such policy and conceptual vacuums are the marks of basic problems within computer ethics. Therefore, computer ethics is a field of substantial practical importance." [Moor(1992)]

Here the logical malleability of computers is taken as the central cause of several effects computers will have on society, and from these effects, the need for computer ethics follows. What we would like to explore, is what ethical issues follow from the aspect of reconfigurability in itself (hence, not from the effects) in reconfigurable technology. Does reconfigurable technology ask for different types of functional and non-functional requirements? Do we need to specify meta-requirements to capture requirements on the level of the reconfiguration process?

An important aspect of reconfigurability is that it challenges the type of stable, knowable, unambiguous function ascriptions to artifacts and systems. The STARS-project, one could say, takes it as a goal to defer the specification of functionalities for the technology past the design phase, even past the implementation phase, to remain flexible during the use phase. In that sense, the central feature of reconfigurability may ask for an extension of existing theories of technical functions. [Houkes and Vermaas(2010)]

This clearly bears on the principle of informed consent. A prerequisite of that principle is a knowable impression of what the system will do under which circumstances. One can argue that this prerequisite is hard to fulfill for many of todays (socio-technological) systems, as they are developed for a certain goal, but once in place, easily used for or combined with other functionalities. This is called function creep; a well known example is the use of cameras introduced to implement a road pricing system (also) for the detection of stolen cars, or tax evaders. But the issue is even more prominent if the system is intended to be reconfigurable to changing circumstances, and maybe even designed to fit yet unthought of functionalities and affordances.[1] At what level of abstraction can the system's behavior be specified for people subject to it, and is that enough of a basis for them to be able to consent or as a basis to justifiedly assume their consent?

The specification of the behavior of the system requires a sophisticated and complex balancing of the different goals the different functionalities of the technology serves. Combining technology for flexible and multiple functionality into one sensor, adds the restriction that only one functionality at a time can be actually used: as mentioned before, concurrent use of different functionalities may not be possible. This means that more crucially than usual, priorities of the different functions must be assigned. This adds an extra dimension to the design process, namely the necessity of designing policies to specify priorities. But these policies should also be flexible to deal with the flexible functionality of the technology.

We should disentangle two sources of complexity: the technical complexity raised by the reconfigurability (which is deterministic), and the complexity associated with the fact that the application of the technology is deliberately left open (which is even non-monotonic). The latter will be the biggest challenge to address. Indeed, the observations above show that the reconfigurability leads to an increased range of choices that need to be made. These choices address not only practical aspects, but more essentially higher order choices: who will be in control of such (practical) choices? Who will bear responsibility for the different functionalities, or for the system as a whole? This indicates that the development of policies around reconfigurable systems will bring in new complexities. Such complexity may compromise the expected efficiency of reconfigurability.

5 Reconfigurability in context?

Even though the project may be envisaged for use as a *closed* system, in the sense that the network will be closed and the

[1] One could jokingly call this: "function-creep-by-design".

users will be more or less stable (order preserving authorities, such as fire fighters, police, port authorities), the problem with the reconfigurability is the openness of the contexts in which the technology may be used.

Although the initial use case for the reconfigurable sensor networks is not primarily related to the observation of persons and their behavior, we deem it useful to look at the ethical issue related to sensor networks like camera surveillance and RFID access control systems. There is extensive literature discussing how sensor networks for observation of individuals and their environment bring up issues concerning privacy and the protection of personal data, such as [Chan and Perrig(2003),Shi and Perrig(2004)], and the legally oriented account in [Solove(2008)]. Despite the fact that the described use case for the reconfigurable sensor networks does not center around privacy, we expect that the technology may in the future be applied in privacy sensitive ways. This not just because the functionality is left open to future use and might include observation of individuals, but also because with increasing data collection surrounding all transactions in society, and linking of databases, objects and transaction traces can be more and more easily linked, also to people. This means that object data may turn into personal data a posteriori. But besides that, we argue that central notions from the discussion of privacy may be helpful in the analysis of reconfigurability, in particular the notion of *context*.

Reconfigurability puts the context of use and control of information, captured in notions such as ‘spheres of justice’ or ‘spheres of access’ [Hoven(1999),Nagenborg(2009)] and ‘contextual integrity‘, as used by [Ackerman et al(2001)], [Nissenbaum(2010)], even more crucially at the heart of the challenge put forward by privacy. For example, Nissenbaum understands privacy in terms of context-relative information norms, and distinguishes norms of appropriateness, and norms of distribution. She defines contexts as “structured social settings, characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).” [Nissenbaum(2010), p.132-134] Most relevant to the framework of Contextual Integrity are the roles, activities, norms and values. For reconfigurable systems there may be different roles, activities, norms and values that need to be combined in the design of one system, and its usage policies. How to deal with the composition of these different contexts for one system is a particular challenge.

Reconfigurability involves applicability of one system with multiple functionality in possibly distinct contexts. In the case of reconfigurable sensor networks, the challenge will be to formulate requirements that are both general and specific enough to cover each possible use. For example, how to balance privacy issues if the sensor system monitors individuals only in very few of its configurations? And how to go about changes in this configuration? Nissenbaum’s framework for Contextual Integrity provides explanation, evaluation and prescription, and thereby contributes to the design process. However, it does not “support substantive descriptions for general families of technologies”, and “the most fruitful assessments take place within particular contexts” [Nissenbaum(2010), p.190]. In the case of reconfigurable systems, the particular context may be underspecified, or only one of a vast number of possible contexts. Therefore, a specific challenge for design for values of reconfigurable technology, such as sensor networks, requires an analysis of the composition and interaction of different contexts, and its translation into policies.

6 Concluding remarks and future work

In this paper we presented an initial, mostly conceptual reflection on the challenge that reconfigurable technology poses to design for values. Reconfigurability of sensors in networks seems to be an attractive answer to the increasing and invariably changing demands in the security and crisis management domain, both in terms of economy and of effectivity. In the coming years, with the progress of the STARS-project we will develop a more thorough analysis of the concept.

The central aim behind the reconfigurability of the technology developed in STARS is to keep the use of the technology open to future functionalities, uses that are not explicitly envisaged yet in the design phase of the technology. in other words, the technology is designed to give the affordance to address future, yet unknown, applications by making the technology reconfigurable. *Function creep* is replaced by the explicit goal of *function shift* towards yet undefined functionalities. Configurations could change overnight towards new functionality - but how do people subject to it or using it get to know this? Reconfigurability thereby implies that there is uncertainty about what the current normative framework is (which is an epistemic problem).

Although at first sight, one could say that the sensor networks of STARS are intended to be closed systems, in the sense that the amount of user parties is limited and coordinated, reconfigurability gives the sensor networks open traits of a slightly different kind. The openness towards its functionality makes that systems’ role based access models should also be reconfigured with the system. This contributes to the non-technological complexity of reconfigurable technology, an aspect which is not to be overlooked.

We note that even if the STARS-sensors are not primarily intended for monitoring persons, privacy may become an important ethical issue to take into account when designing the technology. One has to be aware that the what counts as ”personal data” is being stretched by the development of ”the internet of things”: by connecting data, data gathered about objects are easily linked to (data about) people, and thereby transitively become personal data after all. Furthermore, the fact that privacy is a human right, makes it always a juridical constraint. The European Union expects from companies and research consortia to take their own responsibility (*responsible innovation*): they should be able to justify how they dealt with constraint/secured values.

It will be interesting to see how reconfigurability can be analyzed from the perspective of the literature on function ascriptions and requirements engineering. Is (physical) reconfiguration essentially different from reconception of the possible use of a piece of technology? We believe that a proper analysis and definition of context and spheres will be crucial in the “design for values” of such technology: it is essential both for understanding its potential effects and, in practice, for the formulation of usage policies.

References

[STA(2010)] (2010) Stars project information. Retrieved from STARS-Project website: http://starsproject.nl/.

[Ackerman et al(2001)] Ackerman M, Darrell T, Weitzner D (2001) Privacy in context. Hum-Comput Interact 16:167–176

[Brey(2011)] Brey P (2011) Anticipatory technology ethics for new and emerging technologies. URL https://spt2011.unt.edu/, presidential address at the Society for Philosophy and Technology conference, Denton TX, USA

[Chan and Perrig(2003)] Chan H, Perrig A (2003) Security and privacy in sensor networks. Computer 36(10):103–105

[Gibson(1986)] Gibson JJ (1986) The theory of affordances, Psychology Press, chap 8, pp 127–143

[Guo(2006)] Guo Y (2006) Mapping applications to a coarse-grained reconfigurable architecture. PhD thesis, University of Twente, Enschede

[Houkes and Vermaas(2010)] Houkes W, Vermaas PE (2010) Technical Functions: On the Use and Design of Artefacts (Philosophy of Engineering and Technology), 1st edn. Springer

[Hoven(1999)] Hoven MJ (1999) Privacy or informational injustice? In: Pourcia L (ed) Ethics and information in the twenty-first century, Purdue University Press, pp 140–150

[Moor(1992)] Moor JH (1992) What is computer ethics?, Southern Connecticut State University, New Haven, CT, USA, pp 1–11. Reprint of Moore, J. (1985). What is computer ethics? Metaphilosophy, 16(4): 266-275.

[Nagenborg(2009)] Nagenborg M (2009) Designing spheres of informational justice. Ethics and Information Technology 11:175–179

[Nissenbaum(2010)] Nissenbaum H (2010) Privacy in Context. Stanford University Press

[Palm and Hansson(2006)] Palm E, Hansson S (2006) The case for ethical technology assessment (eta). Technological Forecasting and Social Change 73(5):543–558

[Shi and Perrig(2004)] Shi E, Perrig A (2004) Designing secure sensor networks. Wireless Communication Magazine 11(6):38–43

[Solove(2008)] Solove DJ (2008) Understanding Privacy. Harvard University Press

[Zhao et al(2003)] Zhao W, Chellappa R, Phillips P, Rosenfeld A (2003) Face recognition: A literature survey. Acm Computing Surveys (CSUR) 35(4):399–458