# Requirements for Reconfigurable Technology: a challenge to Design for Values

F. Dechesne, M.J. van den Hoven, M.E. Warnier

Department of Technology, Policy and Management,
Delft University of Technology, The Netherlands
Jaffalaan 5, 26282 BX Delft
The Netherlands
Tel. +31-15-2785143
Fax. +31-15-2786439

F.Dechesne@tudelft.nl, M.J.vandenHoven@tudelft.nl,
M.E.Warnier@tudelft.nl

**Abstract.**
With the increasing use of information technology for different societal goals, the demand for flexible and multiple-functionality appliances has risen. Making technology reconfigurable could be a way of achieving this. This working paper 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 reconfigurability raises for sociotechnical systems like sensor networks. We foresee that reconfigurable technology adds an extra challenge to the identification and specification of functional and non-functional requirements for the technology.

Keywords: reconfigurability, design for values, sensor networks

## 1 Introduction: the STARS project

This paper is written against the background of a large scale research project in The Netherlands called STARS: Sensor Technology Applied in Reconfigurable Systems. The STARS project is still in its initial phase, and involves both academic and private research partners. The project is motivated by the fact that 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 (like, 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. Especially the application area of security has pushed the development of all kinds of sensor technology.

The goal of the STARS-project is the development of "*necessary knowledge and technology to be able to build reconfigurable sensors and sensor networks*" [14]. 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.

Reconfigurable sensors are developed to have these characteristics. They allow for flexible application, because the functionality enclosed in the system can be altered relatively simply and quickly. In the scenarios that are expected, reconfigurability is used to instantaneously optimize for foreseen situations and the corresponding tasks. In the new, unexpected scenarios, the 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 the police, security- and information services fire brigade 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.

The 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. The role of the authors of the current paper is to evaluate societal and moral implications of the technology that is developed within the STARS-project.

We illustrate these issues in the next section, where we describe a use case from the STARS 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 the identification and specification of functional and non-functional requirements for the technology. Already, the wide applicability of the technology in society (*logical malleability* in Jim Moor's terminology [8]) requires that societal and moral values are considered in the application phase, and ideally also already in the design phase. With the flexibility of reconfigurable technology, this requires new tools. A specification language that is both general and specific enough to cover all possible uses is needed.

## 2 Use Case: Sensor Usage in a Large Mainport

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 mainport: a large port area (for example, the port of Rotterdam or Shanghai). Radar systems are used in large ports to 'follow' 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 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) is 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 can be very useful in such environments, since they can be used 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 very useful in this case, but it also leads to a number of 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. Although the aim is to be almost instantaneously reconfigurable, initial versions of the technology will be likely to need some processing time 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.

All these issues stem from the same core problem: reconfigurable systems have more functionality than normal systems, but they cannot use the added functionality concurrently. One can either search for ships or for low flying planes, not both (at the same time). If different functionalities support different values, who gets to decide which value should be given priority?

## 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 turns out this notion requires a deeper analysis.

The computer (the 'universal machine') possibly seems the most obvious example of reconfigurable technology. In his seminal paper *"What is Computer Ethics?"* [8], 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."* [8]

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?

We think it is important to distinguish flexible functionality from flexible configuration: the relationship between them deserves some more detailed study (also beyond this paper).

Literally "*reconfiguration*" means: to modify the configuration, i.e. the arrangement of the parts (of a system). The use of computers has extended functionality of sensor systems already, for example the enhancement of CCTV systems with software that processes faces and compares these to a database with known subjects 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 not every alteration or extension of *functionality* is necessarily a reconfiguration. In the case of adding computers for information processing in a sensor network, this is not just a rearrangement of existing parts of the system, but *adding* elements to the system. Furthermore, reconfigurability is not essential for a piece of technology to have multiple functionality: the same piece of technology may have very different functionalities depending on how and with which intention it is used. An example of this is a plane: usually a means of transportation, but can be used as a highly destructive explosive in the hand of terrorists without any adaptations to the configuration.

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 will involve mainly analogous front-ends (infrared, radar, etc.) and digital signal processing. We think the resulting range of 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 raised by making parts of the architecture reconfigurable, such as those concerning testing procedures, software-hardware partitioning and composability (as pointed out for software architecture in [4]).

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-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 (like *Ethical Technology Assessment* [11] or *Anticipatory Technology Ethics* [2]).

## 4 Reconfigurability as a challenge for design for values

An important aspect of reconfigurability is that it challenges the type of stable, knowable, unambiguous function ascriptions to artifacts and systems. In that sense, it may ask for an extension of existing theories of technical functions. [5]

This 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 today's (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 fit for yet unthought of functionalities. At what level of abstraction can the system's behaviour 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 behaviour of the system requires a sophisticated and complex balancing of the different goals the different functionalities of the technology serves. Combining technology for multiple-functionality into one sensor, adds the restriction that only one functionality at a time can be actually used: as mentioned above, the functionality may not be usable concurrently. This means that more crucially than usual, priorities of the different functionalities must be assigned. This adds an extra dimension to the design process: the specification of priorities.

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.

A fundamental question that should be asked whether the (physical) reconfiguration of the technology is in fact essential for the issues we relate to reconfigurability. Without actually reconfiguring the technology, we can already conceive of certain technology to be used for something else. Think of a car or a plane that can be used for terrorist attacks rather than for transportation, or the use of nuclear technology for the development of weapons rather than for the generation of electricity (*dual use*). Sometimes it just takes another perspective towards the technology in order to enable different functionality. Can we distinguish between ethical issues related to the (intended) reconfiguration of technology and (unintended) (re)perception of the functionality of certain technology (without being reconfigured)?

Although the initial use case for the reconfigurable sensor networks is not primarily related to the observation of persons and their behaviour, 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, e.g. [3,12,6,13]. 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. But besides that, we argue that central notions from the discussion of privacy may be helpful in the analysis of reconfigurability.

Reconfigurability puts the context of use and control of information, captured in notions like 'spheres of justice'/'spheres of access' [7,9] and 'contextual integrity' [1,10], 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).*" Most relevant to the framework of Contextual Integrity are the roles, activities, norms and values. [10, p.132-134]. For reconfigurable systems there may be different roles, activities, norms and values that need to be combined in the design of one system. 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*". [10, 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, like the sensor networks, requires an analysis of the composition and interaction of different contexts.

## 5 Conclusion

Reconfigurability of sensors in networks seems to be an attractive answer to the increasing and unvariably changing demands in the security and crisis management domain, both in terms of economy and of effectivity. In this paper, we have presented an initial exploration of challenges reconfigurability may add in the ethical analysis of technology. In the coming years, we will develop a more thorough analysis of the concept. 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 (like in *dual use*)? We believe that a proper analysis and definition of context and spheres will be crucial in the 'design for values' of such technology, and essential for understanding its effect.

## References

1. Ackerman, M., Darrell, T., & Weitzner, D. (2001). Privacy in context. *Human-Computer Interaction, 16*, 167-176.
2. Brey, P. (2011), *Anticipatory Ethics for New and Emerging Technologies*, Presidential address at the Society for Philosophy and Technology conference, Denton TX, USA, May 27, 2011 (https://spt2011.unt.edu/).
3. Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer, 36* (10), 103-105.
4. Guo, Y. (2006). Mapping applications to a coarse-grained reconfigurable architecture. PhD-thesis, University of Twente.
5. Houkes, W., and P.E. Vermaas (2010) Technical Functions: On the Use and Design of Artefacts, vol. 1 of *Philosophy of Engineering and Technology* (Dordrecht: Springer).
6. Hoven, J. v. (2008). Information Technology, Privacy, and the Protection of Personal Data. In J. v. Hoven, & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 301-321). Cambridge University Press.
7. Hoven, M. J. (1999). Privacy or informational injustice? In L. Pourcia (Ed.), *Ethics and information in the twenty-first century* (pp. 140-150). Purdue University Press.
8. Moore, J. (1985). What is computer ethics? *Metaphilosophy, 16(4): 266-275.* Retrieved from http://www.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html (June 16, 2011)
9. Nagenborg, M. (2009). Designing spheres of informational justice. *Ethics and Information Technology , 11* (3), 175-179.
10. Nissenbaum, H. (2010). *Privacy in Context.* Stanford University Press.
11. Palm, E. & Hansson, S.O. (2006), The case for ethical technology assessment (eTA), *Technological Forecasting and Social Change*, 73(5), 543-558.
12. Shi, E., & Perrig, A. (2004). Designing Secure Sensor Networks. *Wireless Communications, 11* (6), 38-43.
13. Solove, D. J. (2008). *Understanding Privacy.* Harvard University Press.
14. STARS. (2010, July). Project Information. Retrieved from STARS-Project website: http://starsproject.nl/