Development of a Specification for Data Interchange Between Information Systems in Public Hazard Prevention: Dimensions of Success and Related Activities Identified by Case Study Research

Simone Wurster, Department of Innovation Economics, Berlin University of Technology, Berlin, Germany

ABSTRACT

Standards and specifications for public security are missing in many technical aspects as well as the areas of communication protocols and security management. Several research gaps related to these fields exist, particularly regarding R&D stage standardisation. Sherif et al. (2007) offer a framework to investigate project management aspects leading to successful standardisation. Its applicability for R&D stage security standardisation was examined and mainly proved by a recent InfraNorm survey in the German security research program. The German project InfraNorm aims at initiating the development of standards and specifications for the protection of transportation infrastructure. This article gives insight into the development of such a specification based on R&D results. Besides providing practical examples for activities related to Sherif et al.’s (2007) framework, the article suggests its extension. Standardisation challenges and solutions are also unveiled. The article finishes by outlining key aspects which may influence the adoption of the specification and by giving a short overview of current results. Application fields of the findings include, in particular, fast track standardisation procedures with voluntary implementation of the results, standardisations of R&D results and standardisation projects from small groups.

Keywords: (DIN SPECS) Deutsches Institut für Normung Specifications, InfraNorm, Public Security, R&D Stage Security Standardisation, Standardisation

DOI: 10.4018/jitsr.2013010103
1. INTRODUCTION

1.1. Public Security, Standards and Standardisation Needs

The global intensity and frequency of terrorist attacks since the turn of the century show the vulnerability of modern societies and the need for protecting so-called critical infrastructures in particular (see Kuechle, 2009). Several recent studies highlight the need for security-related standards, e.g. DIESIS (2012), ECORYS (2009), ESRIF (2009), the European Commission (2008), the European Council (2010) and Sáez et al. (2009). Standards and specifications for public security are missing in many technical aspects, as well as the areas of communication protocols and security management.

Sinay (2011) defines security as ‘a system of measures, including their embodiments and their interactions, designed to ward off intentionally destructive activity resulting in injury or material damage’. The current global market size for security technologies and services is estimated at 100 billion Euros (approximately 143 billion US dollars), and the annual growth rate is predicted at a minimum of approximately 5% for the next few years (see ECORYS, 2009).

Standardisation is ‘the activity of establishing and recording a limited set of solutions to actual or potential matching problems directed at benefits for the party or parties involved balancing their needs and intending and expecting that these solutions will be repeatedly or continuously used during a certain period by a substantial number of the parties for whom they are meant’ (de Vries, 1999, p. 13).

Specific standards on national level will be described in the next section by explaining fast track standardisation procedures in Germany.

Blind (2004), as well as Swann (2000, 2010), offers an extended overview of the many advantages standardisation provides for the parties involved. To stimulate lead markets for security-related technologies and services, standards and specifications may provide knowledge and technology transfer, connect relevant stakeholders, foster innovative demand, provide innovation-enhancing regulatory frameworks, intensify competition and increase exportability (see Blind, 2008a).

Although some researchers are closely involved in standardisation processes, the vast majority of scientists (not only in the security field) seldom regard standardisation as a high priority. Either they enter the standardisation arena too late or standardisation is neglected in favour of scientific publications or patent applications (see Blind and Gauch, 2007). As a result, many researchers do not use the special opportunities that standardisation can offer them. Numerous benefits of standardisation have been described above. Standards can often facilitate the development of a much larger market for a technology than a company as an individual can realize solely based on proprietary specifications. Some R&D managers know this, but there are still too few (see Blind & Gauch, 2007).

InfraNorm is a joint project between the DIN German Institute for Standardisation and the Berlin University of Technology (duration: March 2010 – February 2013). It belongs to the research area ‘Protection of transport infrastructures’ of the German Framework Programme - Research for Civil Security and is funded by the German Federal Ministry of Education and Research. Its goal is to initiate the development of standards and specifications for the protection of transportation infrastructure based on R&D stage standardisation.

InfraNorm collaborates with ten associated project consortia, initiated to improve the protection of airports, train stations and ports as well as the protection of railways, bridges and tunnels. They are comprised of approximately 80 partners altogether. A specific work package aims at developing a standardisation manual for the participants of the German security research program. Its completion relies on a multi-method approach including several case studies of security standardisation projects.
The Perils of Access and Immediacy: Unintended Consequences of Information Technology
www.igi-global.com/chapter/perils-access-immediacy/29305?camid=4v1a