Unlocking Access: Optimizing Physical Access Control Policy by Smartly Utilizing Employee Attributes

Christina Keysers, Industrial Design Engineering, University of Twente, The Netherlands

In the project, it is investigated how smartly utilizing employee attributes can simplify the setup of physical access control within big organizations. The aim is to automate and enhance the control policy while maintaining system transparency and insights. For this, a systematic model of the control system is developed with the help of applied research.

The assignment was obtained at Nedap N.V., a technology company which does develop people-centred software and hardware solutions, which is also well-represented by their slogan "technology for life". Their mission is to enhance and innovate technologies that assist individuals in their professional lives. The outcomes of this research aim to enhance security policies by increasing efficiency and effectiveness, and therefore simplifying the lives of employees and security personnel alike.

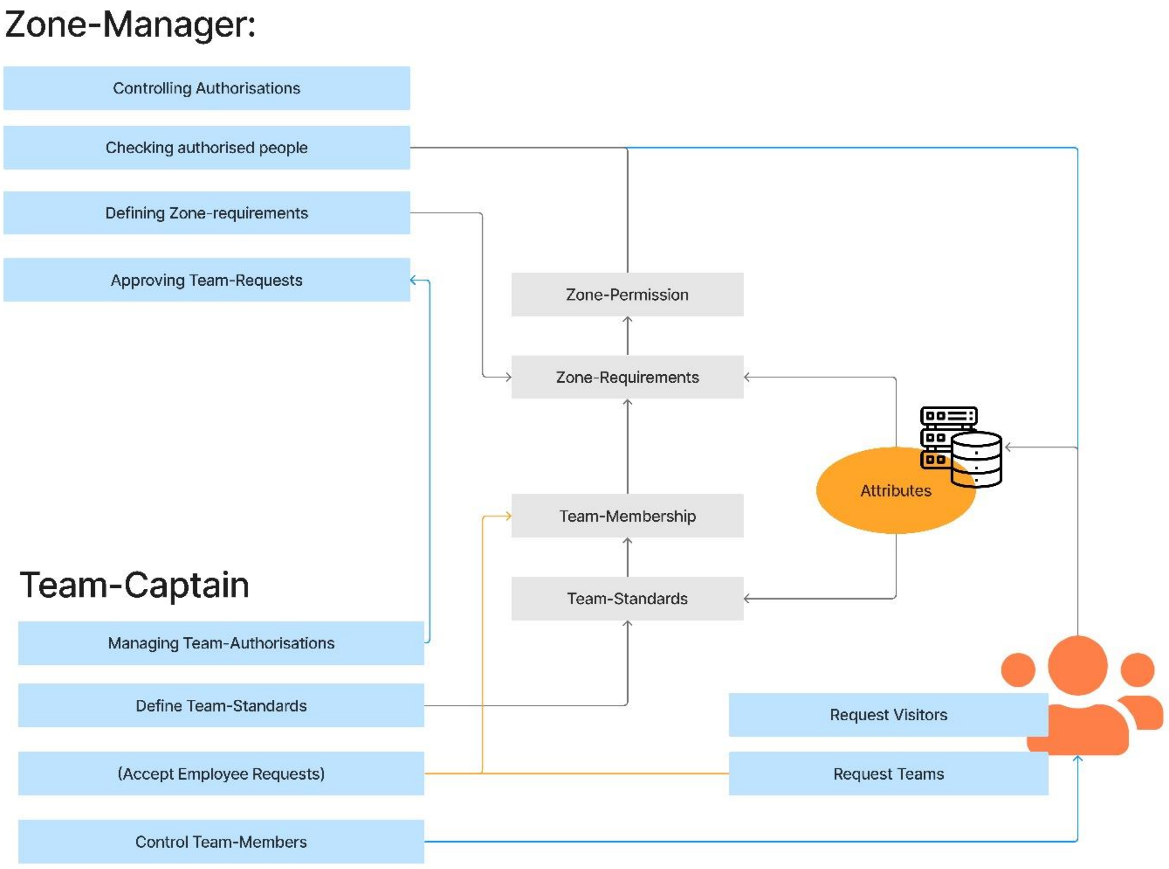
The applied research conducted involved company intern expert interviews to gain insights into the client's value proposition and their existing product. Literature research was conducted to understand the structure and general requirements of physical access control systems, and external customer interviews were carried out to investigate user needs and preferences for such a system. With these insights, key requirements for the system were formulated.

Based on these requirements the first iteration process took place. Throughout the design process, concepts were iterated upon and further developed based on continuous client and customer feedback. This iterative process resulted in the development of a systematic model that is primarily visualized through the creation of a User-Interface. The User-Interface also can be used to evaluate the system's transparency and intuitiveness.

The final model can be described as an attribute-role-based physical access control system implemented within the existing team and zone structure of the software. This team- and zone structure states that teams grant access to zones, rather than individuals granting permissions to operate doors. This approach differs from other access control systems. The term 'role-attribute-based' does implement the use of employee attributes to identify access permissions and role definitions. Role definitions in this system are identified by team memberships.

Automation capabilities and the introduction of authority roles were incorporated to enhance the system. The roles introduced in this concept are the Team-Captain and the Zone-Manager. The Team

-Captain ensures access to required zones for the team and manages team members. They hold the option to automate team member assignments by employing an attribute-based rule engine which can be defined by so-called ‘team standards’. The zone manager is responsible for managing access rights to physical zones, controlling individuals with access permissions, and defining access requirements for zones of accountability. Assigning a zone manager enhances the system's safety by assigning human responsibility for a physical zone. Furthermore, an application with a simplified interface was developed to enable employee operations, such as reviewing access rights and requesting team memberships.



The systematic model designed enhances the control policy rather than automates it, is based on customer desires and the client's value proposition, and fulfils needs identified during literature research. The limited automation capabilities are based on safety constraints and the desire to uphold human accountability. Thus, it can be concluded that the process is effectively addressing the problem statement. Further development of this concept requires quantitative research to validate the implemented functions, assess technical feasibility, and identify missing components.