Smart Construction Sites - Proof of Concept

Introduction

Using 'smart' technologies, we create a more efficient, safer and clearer working environment on construction sites. Several solutions are developed to improve construction practices. These methods allow for lower project costs, more sustainability, better overview, ...

These 'smart' technologies are not limited to automating various processes, but ensure massive connectivity. This leads to the concept of 'track-to-order', which is nothing more than several cameras placed around the inventory to check which items must be ordered to adjust this inventory. We also make sure that when things are taken out of the inventory, this is recorded in a database, to check which project teams have used it. This way, we can more easily find out the cause of the disappearance of the product in case of theft.

Inventory

Our biggest asset is 'circularity' where we operate on the basis of fully connected process management. Digitizing and taking stock of material management has positive consequences in the field of labour productivity. Camera tracking ensures that all items taken from inventory and those brought back are stored in a database. Each material removed from inventory is linked to the team in question in the database. This ensures that we can check at any time if they are indeed active on the site in question. This is made possible by the fact that these cameras track all materials, machines and other items at each site. In this way, the site manager can also know which materials are currently at the site.

All information that a project team needs at the start of the project, i.e. the necessary materials, machines, etc., is sent to the database. Together with the inventory database, this will check if there are various items that are currently out of stock. If this is the case, new items will be purchased.

Benefits

By applying these systems, we can ensure that unnecessary purchases are made if different equipment/materials are not on site. If equipment is broken, new equipment will be purchased immediately and the inventory will be updated. By clarifying the 'exact' location of the various materials clear, there is a clear view of the distribution. This will also bring benefits in terms of safety, which will be discussed later.

Efficiency

Too often looking for tools, equipment, materials, all these issues are solved by inventory tracking. Employees / employers will have to request information about the quantity that is still present less often. Problem situations are solved conveniently by avoiding any clashes in purchases of products.

Material information, which is made clear in good time for each project. Creates clear planning information about when we will have different materials available.

This way of working ensures that the actual work, being actively present at the work site, can be heavily promoted. Every 3 weeks, the inventory is checked by employees, who check if everything is in place, if items are present or absent, and if this is not mentioned on the list. In this way, we can easily maintain the inventory.

Safety

Increasing safety on building sites and in inventories is a very important concept within smart construction. With the 24/7 active tracking cameras that will track all materials and the data database that keeps track of which team is using these things, we can trace all materials much easier.

Dangerous materials will also be kept out of each other's way in this way. The different risks that can occur have been worked out in the system, which ensures that if a worker with different materials wants to enter a zone, he may receive a notification indicating that there is a high risk on the route, place he is currently in.

GDPR

Smart City projects are using sensitive data and they must comply with GDPR law. GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

There are many guidelines to define standards. These guidelines are defined by ISO (International Organization for Standardization). The following standards apply in Smart Cities:

- General standard:
    - ISO/IEC 27570: Privacy guidlines for smart cities
- Privacy standards
    - ISO/IEC 29100: privacy framework
    - ISO/IEC 29134: privacy impact assestement
    - ISO/IEC 27701: privacy information management system requirements
    - ISO/IEC 29151 code of practice for PII protection
    - ISO/IEC 27550 privacy ingineering
- IoT Standars
    - ISO/IEC 30141 IoT Reference Architecture
- IT governance standards
    - ISO/IEC 38500 Corporate governance of information technology
    - ISO/IEC 38501 Governance of IT-implementation guide
    - ISO/IEC 38502 Governance of IT-Framework and model
    - ISO/IEC 38505-1 Application of ISO/IEC 38500 to the governance of data

Our project is affected by general, privacy and IoT standards.

ISO/IEC 27570 scope (Privacy guidlines for smart cities)

The document takes a multiple agency as well as a citizen-centric viewpoint.

It provides guidance on:

- — smart city ecosystem privacy protection;
- — how standards can be used at a global level and at an organizational level for the benefit of citizens; and
- — processes for smart city ecosystem privacy protection.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.

ISO/IEC 29100 scope (privacy framework)

This International Standard provides a privacy framework which

- — specifies a common privacy terminology;
- — defines the actors and their roles in processing personally identifiable information (PII);
- — describes privacy safeguarding considerations; and
- — provides references to known privacy principles for information technology.

This International Standard is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

ISO/IEC 29134 scope (privacy impact assestement)

This document gives guidelines for

- — a process on privacy impact assessments, and
- — a structure and content of a PIA report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

This document is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.

ISO/IEC 27701 scope (privacy information management system requirements)

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

ISO/IEC 29151 scope (code of practice for PII protection)

This Recommendation | International Standard establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII).

ISO/IEC 27550 scope (privacy ingineering)

This document provides privacy engineering guidelines that are intended to help organizations integrate recent advances in privacy engineering into system life cycle processes. It describes:

- — the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and
- — privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and architecture design.

The intended audience includes engineers and practitioners who are involved in the development, implementation or operation of systems that need privacy consideration, as well as managers in organizations responsible for privacy, development, product management, marketing, and operations.

ISO/IEC 30141 scope (IoT Reference Architecture)

This document specifies a general IoT Reference Architecture in terms of defining system characteristics, a Conceptual Model, a Reference Model and architecture views for IoT.