

Integrating UPnP technology with CAFM systems – automated device identification and device control in building operation and maintenance

1

Asbjörn Gärtner and Björn-Martin Kurzrock

Department of Civil Engineering, RPTU University, Kaiserslautern, Germany

Received 12 April 2024
Revised 22 September 2024
Accepted 4 October 2024

Abstract

Purpose – Modern buildings use intelligent automation for comfort, efficiency and sustainability, impacting their construction and operation. Although building automation (BA) operates via bus lines and is controlled by sensors and actuators, computer-aided facility management (CAFM) systems often handle data redundantly. Current standards fail to detail effective systems integration, with a noticeable gap in practical network models and solutions. The purpose of this paper is to design a network model that integrates building services and networks at the automation level. The goal is to enable the CAFM side to control all electrical loads (such as lighting, blinds, pumps), climate control (HVAC) and security monitoring.

Design/methodology/approach – This paper explores the automatic discovery and integration of BA devices and centralized controls into CAFM systems, focusing on innovative networking models, system data provisioning, import functions and web operation. Established technologies such as Universal Plug and Play (UPnP) and Extensible Markup Language (XML) standards are utilized to develop new solutions.

Findings – The paper introduces a solution with a database and software module enabling bidirectional web-based coupling via LAN. The UPnP standard was enhanced to include facility management (FM)-specific information for device communication. The prototype effectively controls devices through CAFM systems, setting a foundation for future improvements in web-based BA. These results are crucial for developing standards for automated data processing between CAFM systems and BA.

Practical implications – This research benefits FM, especially in maintenance, operations, energy and compliance. In addition, the need for time-consuming on-site inspections to record device master data for maintenance management, in case of commissioning or changing facility service providers, can be eliminated. The principles of the developed software module enhance CAFM systems as high-performance building control tools.

Originality/value – The paper adapts existing technologies for specific FM applications and integrates them for the first time into key FM processes.

Keywords Facility management, Building operation, Building automation, Maintenance management, Interface, Device control, CAFM, BA, BACS, UPnP, Plug and play, XML

Paper type Research paper

© Asbjörn Gärtner and Björn-Martin Kurzrock. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>

The Open Access publication of this book was financially supported by the Open Access Publication Fund of the RPTU University.



1. Introduction

Modern buildings rely on intelligent automation technologies for comfort and efficiency, primarily through building automation and control systems (BACS) and computer-aided facility management (CAFM) systems. These systems are crucial for managing large property portfolios (Koch *et al.*, 2019, p. 292, Jaspers *et al.*, 2018, pp. 337–375, May and Williams, 2017, p. 635).

Although few comparative studies have examined the networking of these systems from a facility management (FM) perspective, CAFM systems offer potential for technological integration, including interfaces with enterprise resource planning (ERP), computer-aided design (CAD), or building information modeling (BIM) systems. Currently, CAFM interfaces are mainly unidirectional, facilitating data transfer like meter readings. Expanding control mechanisms requires hardware and software evaluation. CAFM systems use (W) LAN with Transmission Control Protocol/Internet Protocol (TCP/IP), whereas building automation (BA) devices typically use proprietary fieldbus systems.

BACS and CAFM systems differ in both network and data technology, often leading to redundant data storage. This redundancy raises costs and complicates management. A unified IT infrastructure could reduce costs and improve system management.

Furthermore, technical equipment data are still recorded manually, with limited data exchange.

The lack of standards for system integration highlights the need for a solution concept focusing on standardization and process modeling. Centralized data management and control via CAFM remains unachievable, with missing cross-manufacturer and cross-trade standards. These gaps must be addressed by what needs standardization and which processes should be modeled.

2. Aim of the research

The current state of today's implementations necessitates developing a concept for coupling BACS and CAFM systems, eliminating redundant database content, making manual recording and registration of devices for asset and maintenance management obsolete and facilitating web-based control for facility managers via CAFM systems. This concept should set the groundwork for new standards allowing devices to connect regardless of previously considered network technologies.

The approach should simplify the integration, installation and configuration of building equipment, enabling devices to be automatically recognized and integrated into the CAFM system as a "plug and play" feature. System data from technical equipment should be automatically captured during installation and updated via an IP-based, bidirectional link, eliminating the need for separate fieldbuses for classic BA and facilitating active data exchange through the LAN.

Developing and demonstrating these interface functions, particularly for automatic discovery and master data import of devices via LAN (which is not supported by protocols such as Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) and Open Platform Communications Unified Architecture (OPC UA) according to Jaspers *et al.*, 2018), requires programming a database connection and a web interface, showcased in a prototype.

The paper outlines control methods for electrical loads such as lighting, blinds, pumps and heating, extending to indoor climate control and security systems such as CCTV, using a CAFM system. The goal is to design a network model that integrates building services and networks at the automation level, previously only managed at the management level. Standardizing protocols and automatisms in the network is crucial for enabling web-based control without separate fieldbuses and linking to a CAFM database (as a single source of truth for devices), ensuring smooth and automatic master data import via LAN.

3. Research approach

There is a large amount of literature on digitalization in real estate and FM, especially on the use of Internet of Things (IoT) devices and sensor technology, such as [Kastner \(2008, 2016\)](#), [Jaspers *et al.* \(2018\)](#), [Schuster *et al.* \(2018\)](#) and [Redlein and Höhenberger \(2020\)](#). In addition to describing the use cases and application areas, the authors detail how these devices are integrated via interfaces and communicate with each other or with CAFM/IWMS systems using various protocols. However, there is no discussion in the literature about the existing technology – established in the field of multimedia devices – for automatically discovering and registering these devices in the network and for importing device master data (device and service description) provided by the manufacturers, as is the case with Universal Plug and Play (UPnP). This approach is new.

The work arises from CAFM implementation projects, highlighting the need for automated device recording and identification. Detailed in a requirements analysis, the concept includes automatic device registration within the network and transferring information to a CAFM database, elimination time-consuming on-site inspections to record device master data, which often occurs before commissioning or when changing facility service providers.

The approach utilizes existing technologies and standards to develop new solutions. Initially, system integration options are explored and assessed using hardware interface models. Model evaluations prioritize the most suitable option based on key criteria. After defining the setup and network structure, the technical execution of the prototype is detailed, with processes illustrated as a workflow model. Standards are then established for vendor- and product-independent functionality.

Various coupling variants using different protocols (such as MQTT, CoAP, OPC UA and Multicast Domain Name System [mDNS]) and technologies (such as KNX, BACnet, ZigBee, EnOcean, LoRaWAN, Bluetooth and UPnP) are considered, compared and evaluated. Requirement criteria are validated and ranked with industry partners and assessed in a comparison matrix to identify the superior option. Most technologies are not originally designed to automatically discover the devices on the LAN, so the choice and further consideration fell on UPnP.

The findings lead to the development of a VB.NET module for CAFM systems, with integrated UPnP functionalities. This universal functionality is demonstrated through a prototype application.

The main benefits of combining CAFM and BACS including existing standards (UPnP technology) for facility managers are the avoidance of manual device master data capture through automated device discovery and import of device master data (plug and play), elimination of duplicated data management, homogeneous infrastructure, functional extension of CAFM systems for system control and historical documentation (operator responsibility).

4. State of technology and research

To the authors' knowledge, no research has been published on the automated discovery and coupling of technical building equipment with CAFM systems. Typically, coupling occurs through predefined or customized interfaces provided manually by CAFM system vendors. An entire industry, including the development of the German CAFM standard CAFM-Connect supported by 40 mostly consulting firms ([CAFM Ring, 2024](#)), has emerged around this topic. These solutions often rely on national or specific customer systems. International Facility Management Association (IFMA) and its national chapters, such as the German Facility Management Association (gefma), are working on data exchange standards but have not yet standardized methods. For example, the gefma guideline 470: [gefma, 2017-09](#) on data exchange in FM is under review.

4.1 CAFM systems, building automation and interfaces

From an FM perspective, the usage of CAFM/IWMS systems and workplace automation systems is widespread and very high, with thousands of implementations worldwide and millions of users.

Existing interface concepts mainly facilitate data exchange at the management level. Integrating control commands at the field level extends automation to management functions, making CAFM systems central control hubs. This integration places new demands on network capability and device intelligence.

The standardization of CAFM interfaces has accelerated due to increasing demands for interoperability and efficiency in FM. The CAFM-Connect interface and Industry Foundation Classes (IFC) are important for seamless data exchange across systems. CAFM-Connect caters to the German-speaking FM sector, standardizing data and processes to enhance CAFM system integration. Similarly, IFC, a universal model by buildingSMART, facilitates BIM data exchange across software, promoting consistency and enabling more sophisticated automation in building operations.

4.2 UPnP

Since 1996, the Universal Serial Bus (USB) has provided a standard “plug and play” interface in computer technology, eliminating the need for special drivers for each device.

UPnP extends this principle to networks, with standards set by the Open Connectivity Foundation (OCF), previously known as the UPnP Forum (Miller and Van der Beek, 2014). The UPnP Device Architecture specifies Extensible Markup Language (XML)–based device representation and communication protocols between control points and devices. Most IoT devices integrated into LANs already use UPnP to automatically connect to the network (BSI, 2024), but these are primarily used in consumer products such as multimedia, streaming and network devices; UPnP has not yet been integrated into BA devices (especially heating, ventilation and air conditioning [HVAC]) to connect directly to CAFM systems.

The six-step UPnP device connection workflow is described in the UPnP Device Architecture (OCF, 2024):

- (1) *Addressing*: A UPnP device acquires an IP address via Dynamic Host Configuration Protocol (DHCP) by default or manually for identification on the network.
- (2) *Discovery*: The device announces its presence on the network using the Simple Service Discovery Protocol (SSDP). It broadcasts details such as name, type and URL to the multicast address 239.255.255.250, UDP port 1900, in a protocol known as HTTPU.
- (3) *Description*: Devices provide an XML file detailing properties and services. Control points access this file via HTTP to learn about the device’s manufacturer, serial number and related URLs (for control, events and presentation).
- (4) *Control*: Control points send Simple Object Access Protocol (SOAP) requests to the device’s Control URL to execute commands specified in the XML, using the SOAP over HTTP.
- (5) *Eventing*: The General Event Notification Architecture (GENA), an XML-based protocol, enables control points to subscribe to service status updates, eliminating the need to continuously query for status values.
- (6) *Presentation*: This layer offers an HTML-based user interface accessible via the “Presentation URL,” simplifying device interaction beyond SOAP commands and providing similar functions.

5. Solution concept

5.1 Model evaluation

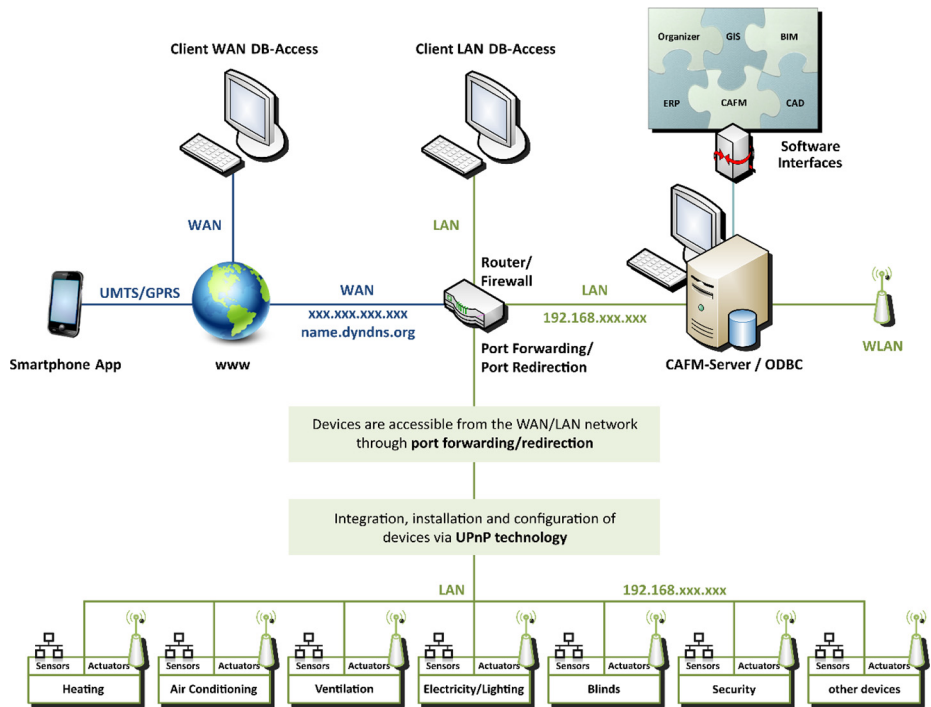
The ten most important aspects in relation to the objective are used for the evaluation of different models. In addition, they are given a weighting of the criterion with a point score that allows for objective prioritization.

- *Pure IP network*: Communication of BA devices via the same network as the CAFM system for importing device master data directly via LAN requires the TCP/IP protocol. Weighting: 3 points.
- *CAFM-based device control*: Crucial is the web-based CAFM system's ability for device-independent and cross-trade control. Standard web capability is assessed. Weighting: 3 points.
- *Seamless device connection via UPnP*: UPnP standard is used for automatic device discovery and registration and data transfer in CAFM and BA. Weighting: 3 points.
- *Wireless integration via WLAN*: Wired connections might not be viable in all environments, making WLAN necessary for UPnP; Bluetooth is unsuitable due to its range and lack of IP protocol support. Weighting: 2 points.
- *Eliminate redundant data storage*: Integration should remove redundant data storage, centralizing attributes in one database. Weighting: 2 points.
- *Cyber security*: Risks of unauthorized WAN access require secure practices such as manual port forwarding and firewall use, with VPN setup being critical. Additional security measures are discussed later. Weighting: 2 points.
- *Cost effectiveness through integration*: Merging management and automation levels improves cost-effectiveness by reducing the need for separate controllers and minimizing hardware. Weighting: 2 points.
- *Database historization*: Essential for tracking user activity and object status via a time-stamped BACS database record. Weighting: 1 point.
- *Automatic generation of maintenance groups*: Maintenance groups are automatically created from XML files with trade categorization attributes. Weighting: 1 point.
- *Simple workflow structure*: Simplifying the workflow aids in understanding and managing communication and data transfer, especially with EnOcean wireless technology (EnOcean, 2024), which uses a chain from sensor to actuator. Weighting: 1 point.

5.2 Superior coupling variant

A bidirectional coupling of IP-based components via LAN emerged from the model evaluation as the superior coupling variant with integrated UPnP technology (Figure 1).

This coupling variant merges management and automation levels by integrating network-capable devices directly into a local network via a router, eliminating the need for control units (Direct Digital Controls, DDCs) or gateways. Devices are identified by their IP address and can be accessed directly on the LAN, functioning as equal participants in the LAN. Access from WAN is also possible through port forwarding/redirection. Communication is based on TCP/IP protocols. Logical processes, scenario switching and control commands, which must be provided by the device itself, are managed centrally by the CAFM server. This variant places new demands on the devices (sensors, actuators).



Source: Author's own work

Figure 1. Bidirectional coupling of IP-based components via LAN

This model fulfils the key requirement for convenient device connection and automated installation – essentially plug and play at IP-network level with UPnP. According to our research, this technology is not yet common in traditional trades such as HVAC. The best known application of this technology is in IP cameras used for surveillance in the security industry. This innovative approach enables easy discovery, registration, installation and direct device control. This requires the definition of protocols and exchange formats. The core of the new standard is the definition of the content of the XML files to be provided.

5.3 Innovative standards

To ensure seamless, manufacturer-independent functionality for all measurement, control and regulation units in BA (I&C technology, sensors and actuators), uniform standards are necessary.

The developed model incorporates standards such as ethernet and WLAN, TCP/IP and the UPnP, including the required XML files. However, integrating these standards with specialized CAFM applications demands specifications for developers and manufacturers to implement the required services, protocols and data formats for UPnP devices.

This specifically includes detailing the structure and content of XML files for UPnP connections and CAFM integration, namely the device.xml and scpd.xml files. Initially, relevant device and service attributes for BA must be identified and organized by function,

control commands and status variables as per the service descriptions. It is also practical to distinguish between data related to asset classes (such as product series/model numbers) and individual asset data (such as serial numbers). The data's origin, whether manufacturer-defined (device properties) or user-specified (location, inventory number, etc.), must also be clearly defined.

Table 1 lists all required attributes for device.xml and scpd.xml files, based on the UPnP specifications, with additional attributes suitable for technical building equipment as identified in our research. Images and datasheets can also be stored on the device for import.

This attribute collection must be integrated into CAFM databases, with corresponding fields appropriately provided. While the recommended names can vary, a mapping table is necessary for importing deviations. This collection supports designing a sample database to demonstrate practical application, with table structures and relationships based on the shown sorting and grouping.

6. Prototypical application

In this section, using the developed coupling model and selected technologies, a simplified relational database model is created along with XML descriptions for UPnP devices and services. This database is central to a prototype web-based application with import and control functionalities.

Due to unavailable BA devices that support UPnP, real operation is simulated, with emphasis on IT infrastructure and software design.

6.1 Structure of the coupling model and technical implementation

The communication process between client, server and devices involves numerous protocol definitions, data telegrams and network access rules.

A CAFM system can be operated locally via LAN or remotely via WAN. For instance, for sending a control command (such as activating air conditioning) remotely, the steps are as follows:

The CAFM system is accessed through an internet browser. User inputs and outputs at the database are managed via SQL commands sent to the CAFM server (which also acts as a web and database server). The server's address comprises the router's IP and a port number. If the IP is not static, a service updates the DNS entries. At the router – the first barrier – the request is forwarded or redirected through the specified port. Once at the server, the values are processed as database entries, queries or control commands and the current field value is returned to the client.

Upon initial use, a new UPnP device automatically registers on the local network and announces its presence. The CAFM server, acting as the control point, recognizes the device and accesses its XML files, initiating the coupling and import process.

6.2 Structure of the database model

All listed attributes must be included in the database model, using the recommended naming conventions with table structures grouped by attribute types.

The database also includes additional tables not supplied by the UPnP-enabled devices or specified by users during import but related to system and maintenance management. These contain data on system locations, maintenance contracts and details about manufacturers or contractual partners.

This database model, however, is only a small, simplified extract for the simulation and not a complete CAFM database with full asset and maintenance management. It serves primarily to demonstrate an import function within the application.

Table 1. Pre- and user-defined properties, services and attributes of device class and device object

	Name	Database field	Source
Properties of device class	Device type	deviceType	UPnP-Standard
	Device name	friendlyName	UPnP-Standard
	Device manufacturer	manufacturer	UPnP-Standard
	Manufacturer homepage	manufacturerURL	UPnP-Standard
	Model description	modelDescription	UPnP-Standard
	Model name	modelName	UPnP-Standard
	Model number	modelNameNumber	UPnP-Standard
	Device homepage	modelURL	UPnP-Standard
	Icon	iconURL	UPnP-Standard
	Service ID	serviceId	UPnP-Standard
	URL of the service description	SCPDURL	UPnP-Standard
	URL of the control unit	controlURL	UPnP-Standard
	URL of the event notifications	eventSubURL	UPnP-Standard
	URL of the device display	presentationURL	UPnP-Standard
	Category number	categoryNumber	UPnP-Extension
	Category name/trade	categoryName	UPnP-Extension
	Category description	categoryDescription	UPnP-Extension
	Maintenance type	mntType	UPnP-Extension
	Maintenance interval	mntInterval	UPnP-Extension
	Maintenance interval time unit	mntIntervalTimeUnit	UPnP-Extension
	Maintenance activities/procedures	mntProcedures	UPnP-Extension
	Weight	deviceWeight	UPnP-Extension
	Length	deviceLength	UPnP-Extension
	Depth	deviceDepth	UPnP-Extension
	Height	deviceHeight	UPnP-Extension
	Width	deviceWidth	UPnP-Extension
Services of device class	Action (service/function)	actionName	UPnP-Standard
	Argument (control command/parameter)	argumentName	UPnP-Standard
	Argument/command direction	direction	UPnP-Standard
	Argument variable	relatedStateVariable	UPnP-Standard
Properties of device object	Serial number	serialNumber	UPnP-Standard
	Universal unique identifier	UDN	UPnP-Standard
	Universal product code	UPC	UPnP-Standard
	Year of manufacture	manufactureDate	UPnP-Extension
	Warranty in months	warranty	UPnP-Extension
	Inventory number	identNumber	user-defined
	Equipment identification code	identName	user-defined
	URL of the device	baseURL	user-defined
	Acquisition cost	retailPrice	user-defined
	Commissioning (date)	startupDate	user-defined
	Maintenance date	mntDate	user-defined
	Maintenance status	mntStatus	user-defined
Attributes of device object	Attribute name	stateVariableName	UPnP-Standard
	Attribute value (at runtime)	stateVariableValue	UPnP-Extension
	Attribute type	dataType	UPnP-Standard
	Attribute default value	defaultValue	UPnP-Standard
	Attribute minimum value	minimum	UPnP-Standard
	Attribute maximum value	maximum	UPnP-Standard
	Attribute level/step size	step	UPnP-Standard
	Attribute event notification	sendEvents	UPnP-Standard

Source: Author's own work

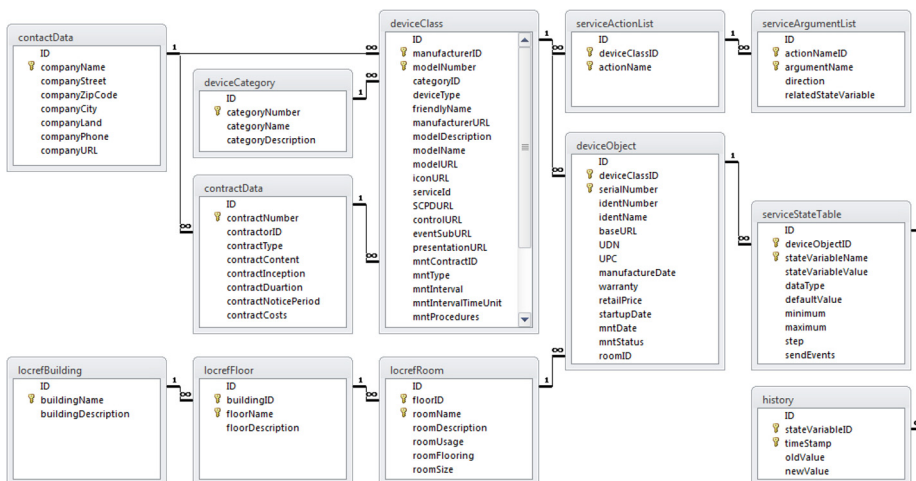
6.3 Structure of database tables and relations

In the initial phase of database design, determining necessary tables and their attributes is crucial. These attributes stem from extended UPnP device and service descriptions. Table names reflect their content and relational database principles such as normal forms are followed to avoid redundant data.

The design is object-oriented, differentiating between a device class grouping similar devices (model-related) and individual objects (e.g. ventilation actuators as instances with serial numbers, while sharing model attributes such as control commands).

Figure 2 outlines the key tables in the relational database structure.

- *deviceClass*: This table includes attributes common to all objects within a class, where “class” refers to a product series or model range. It encompasses model-specific properties, maintenance data, dimensions and weight. Composite primary keys combining manufacturer and product series ensure entry uniqueness. A sequentially numbered ID serves as a reference for relationships to other tables.
- *deviceObject*: Records attributes specific to each device, such as serial number, inventory number and location. A composite primary key of model series and serial number guarantees the uniqueness of each entry.
- *serviceStateTable*: Each device object has service description attributes that define its status, modified by functions (actions). The device object and attribute together form the composite primary key.
- *serviceActionList*: Lists actions or services for a device class. Each combination of device class and action is unique, allowing multiple actions per class.
- *serviceArgumentList*: Each action has associated arguments or control commands, with primary keys formed from the class-dependent action and argument, linked to attributes in the *serviceStateTable*.



Source: Author's own work

Figure 2. Simplified structure of relational database

- *deviceCategory*: Defines device class categorization, referencing trades in a separate table.
- *History*: Records and timestamps changes in status variables to track system control history.

6.4 Structure of XML scheme for UPnP

Once the database has been designed, the device.xml and scpd.xml files need to be created. The XML files are based on the named attributes recommended for a new standard. The templates (device.xml and scpd.xml) for universal devices for technical building equipment are not reproduced in this paper.

6.5 Prototype result: facility automation through integration of BA and CAFM

The following sections present the resulting web-based application (prototype “FMControl”) with database connection for the integration of BA and CAFM systems.

6.5.1 User interface (description)

The prototype’s user interface is accessible via IIS Manager through its specific URL. It is structured to manage space, assets, maintenance, contracts and contact data, with primary focus on asset management. It features an import function and device control methods including device selection or registration, displaying properties and a control section with service attributes and action buttons.

Users can select existing devices, create new ones manually or import devices via UPnP. After selecting a registered device object, the information and control section populates with attributes based on the serial number.

For manually created devices, manufacturer, model number and serial number must be entered to create a unique entry, followed by completing the system description.

UPnP devices are detected on the network and appear in a drop-down menu in the Import section. Selecting a device auto-fills the baseURL field and imports attributes and service descriptions.

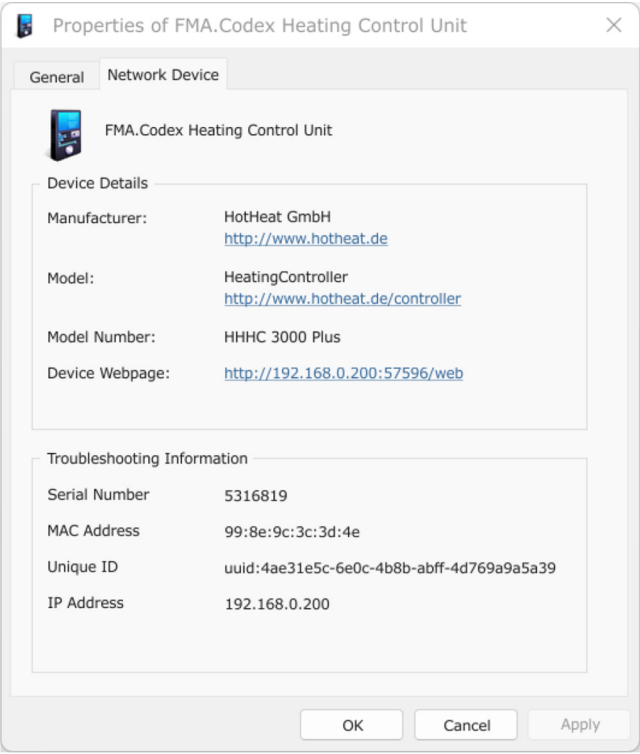
The “Asset/Device Description” section displays a subset of attributes that can be expanded as needed. Manufacturer-specific attributes remain noneditable (indicated as grey fields in [Figure 4](#)).

The “Asset/Device Control” section also includes noneditable manufacturer-defined services. The prototype limits functionality to powering devices on or off, enabling control buttons only if the system state attributes are correctly described. Additional device functions can be incorporated as needed.

6.5.2 Device import (process)

Before importing device and service descriptions, UPnP devices on the network must be discovered, which can be simulated using tools such as the open source “UPnP Developer Tools” (originally by Intel). Detected devices appear as new entries in the Windows Network with context menus displaying their properties ([Figure 3](#)).

All UPnP devices supporting the extended UPnP scheme are listed in a drop-down menu on the application interface. The prototype includes a predefined selection. An unimplemented but advisable routine would filter out previously imported devices. Selecting a device displays its URL, which is required before starting the import.



Source: Author’s own work

Figure 3. Network device properties, screenshot of network device in windows network

The import process reads and writes XML file entries to the “deviceObject” database table in several loops. The imported device is automatically selected, and its information retrieved. [Figure 4](#) illustrates the import result.

User-defined attribute fields start empty (“N/A”) but are editable. Each object can have an inventory number or asset identification key assigned, defined by the user using a trade abbreviation, room reference and a sequential number for multiple same-type devices in one room. For instance, “H.G1401101.1” identifies a heating center in building 14, first floor, room 101.

6.5.3 Device control (process)

The control process is designed for simplicity, operable with a few clicks. Manufacturer-specified properties appear in noneditable fields. The control address shows the URL where the “SetPowerDevice” command is sent to activate the switching actuator. Future adaptations will include a drop-down menu in the “Function” field for selecting device-specific functions, as seen in Figure 4’s “Asset/Device Control” section. System status and range limits are displayed; an additional field for intermediate values may be required. Clicking “Power On” or “Power Off” executes the command and logs it. The control commands originate from the manufacturer’s XML service description via UPnP, imported

FMCONTROL

(c) by AG

Space

Asset/Device

Maintenance

Contract

Company

Asset/Device

Select

Create

Import

Manufacturer

Hot Heat GmbH

Manufacturer

Heating Control Un

Model No.

HHHC 3000 Plus

Model No.

192.168.0.153

Serial No.

121001017

Serial No.

Select

Create new

Import

Asset/Device Description

Device Name

FMA.Codex Heating Control

Inventory No.

N/A

Category

Heating

Ident. Code

N/A

Model Name

HeatingController

Commissioning

N/A

UDN

uuid:0e547a38-a3a6-48df-9

Aquisition Cost

N/A

UPC

UPnP.FMA.Codex.HC.3000

Location Building

N/A

Year of Manufacture

2024-02-14

Location Floor

N/A

Warranty

60 month

Location Room

N/A

Change device data:

Save

Cancel

Asset/Device Control

Control Address

FMA.CodexHeatingService/co

Current Value (On/Off)

N/A

Function

SetDevicePower

Maximum Value / On

1

Control Command

newDevicePowerTarget

Minimum Value / Off

0

Change device status:

Power On

Power Off

Message:

Record inserted successfully.

Confirm message

Source: Author’s own work
Figure 4. Device form after import, screenshot from prototype

into the CAFM system. This XML standard should also include operational and maintenance information.

Each status change is logged with a timestamp and variable reference. This documentation allows filtering and analyzing system statuses for operator accountability or damage assessment.

7. Discussion

The paper aimed to develop a standard for integrating BA technologies with CAFM systems at both the management and automation levels via an IP-based network. The goal was to enable a web-based, database-connected solution for easy “plug and play” integration of BA devices with control features accessible via CAFM. This was demonstrated through a web interface featuring import and historized control functions.

The proposed solution, standard design, database model and application module successfully met all outlined requirements. The database model and the XML service and device descriptions are crucial for establishing standards that will facilitate the development of compatible hardware and ensuring industry adoption.

The interdisciplinary challenge of this project combined knowledge from electrical engineering, IT and FM to design the integration model and innovate by blending BA, CAFM and UPnP technologies.

7.1 Scope and awareness

From an FM perspective, the primary benefit is enhancing CAFM systems with import and control functionalities making them powerful management tools, particularly for energy control. Approximately 36% of companies plan to expand their CAFM systems into areas such as energy management ([gefma, 2023](#)), and about 9% already have data interfaces to BA. Yet, full awareness of the benefits of comprehensive system integration is lacking.

The groundwork has been laid. This concept provides a foundation for programmers and manufacturers to develop UPnP-enabled components or CAFM systems that accommodate necessary services, protocols and data formats. Availability of these components will likely increase demand.

Despite its success, the model has limitations. The pros and cons of the chosen coupling approach are discussed next.

7.2 Pros and cons

Cons: This concept requires every sensor and actuator to be IP network compatible and integrate UPnP service. Due to the absence of UPnP-enabled sensors/actuators in BA, the concept was only demonstrated through software simulations. Device manufacturers are urged to adopt these new standards for data provision.

Unlike energy-efficient EnOcean technology, which operates without external power, this solution requires constant power and uninterrupted network connectivity.

The use of IP-based networks introduces cybersecurity risks, such as malware, Distributed Denial of Service (DDoS) attacks and unauthorized data access ([Kost, 2024](#)). IoT devices integrated into LANs often connect to the internet independently by configuring routers on the network via UPnP to create port forwarding ([BSI, 2024](#)). Ensuring security requires significant IT resources, as the system must adhere to high security standards to protect WAN- or LAN-connected devices from manipulation.

Pros: This solution enables CAFM-based control of UPnP-enabled building equipment via an IP-based network, with automatic address assignment through DHCP.

The automatic import of XML file attributes provides essential information for categorizing devices and generate maintenance groups to enhance system and maintenance management. This ensures no components are overlooked, with error checking through additional import queries or plausibility checks.

Another advantage is the database connection, which records and archives user activities or object statuses with timestamps, supporting operator accountability.

UPnP technology uniquely supports easy, convenient plug-and-play connections in local networks, offering significant potential when integrated with other IoT devices or machine learning algorithms ([Bodenbender et al., 2019](#), 177–178; [Ritter et al., 2019](#), 399–402).

7.3 Security

To enhance UPnP security, network segmentation is recommended to restrict access to sensitive areas, and UPnP devices should regularly update with the latest security patches. Firewalls, secure VPN access and manual port sharing/redirection are advisable. Routers must actively monitor incoming UPnP traffic, and network tools should detect abnormal activity. Devices that support advanced security features such as authentication and encryption are preferred.

Research on Secure UPnP, presented in 2020 but not yet standardized, highlights UPnP vulnerabilities, particularly in service discovery and access within IoT networks. [Kayas et al. \(2020a, 2020b\)](#) developed a capability-based security model that protects UPnP service discovery and access, validated against attacks with minimal performance impact.

8. Conclusions

The findings of this paper establish a foundation for advancing technical building equipment and systems. For practical application and effectiveness, further steps are suggested.

The developed device and service descriptions should be proposed to the OCF for a new “FM automation” section of the UPnP Service Scheme. Instead of a universal template, specific templates for different trades could be created. FM associations such as gefma and IFMA could help disseminate these results to the FM sector.

The prototype currently offers only the “SetDevicePower” function for turning a device on and off. While proof of concept is established, additional functions for future UPnP devices are necessary. The goal is CAFM-side control of all electrical loads (such as lighting, blinds, pumps), climate control (HVAC) and security monitoring.

The database is aligned with service and device description specifications, but integration with existing CAFM systems may require extra fields and translation routines.

It is advisable to establish binding specifications for category naming, using standards such as VDMA, AMEV or DIN 276 in Germany as references for the “categoryName” field in the UPnP standard.

Device manufacturers are encouraged to develop and market UPnP-enabled components. The “FMControl” prototype demonstrates the feasibility of software- and database-supported integration and control.

Long-term development should enhance comfort, safety and energy efficiency, positioning the solution as both a technical innovation and an economically and environmentally sustainable option, potentially supported by certifications like DGNB, LEED or BREEAM.

References

- Bodenbender, M., Kurzrock, B.-M. and Müller, P.M. (2019), “Broad application of artificial intelligence for document classification, information extraction and predictive analytics in real estate”, In: *Journal of General Management*, Vol. 44 No. 3, pp. 170-179.
- BSI (2024), “SYS.4.4 allgemeines IoT-Gerät”, (Edition 2023), available at: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_4_4_Allgemeines_IoT_Geraet_Edition_2023.html
- CAFM Ring (2024), “CAFM-Connect unterstützer”, available at: <https://cafm-connect.org/unterstuetzer>
- EnOcean (2024), “Ultra-low power management”, available at: www.enocean.com/de/technologie/ultra-low-power-management
- gefma (2017), “GEFMA-Richtlinie”, *Datenaustausch im Facility Management*, Vol. 470 2017-09. gefma.
- gefma (2023), “GEFMA 945 - CAFM/IWMS trendreport 2023”, gefma.
- Jaspers, E., Härtig, M., Hofmann, M., May, M. and Turianskyj, N. (2018), “IoT im FM”, in May, M. (Ed.), (2018) *CAFM-Handbuch. Digitalisierung im Facility Management Erfolgreich Einsetzen*, 4th edition, Springer Vieweg, pp. 337-375.
- Kastner, W. (2008), “Gateway-free integration of BACnet and KNX using multi-protocol devices”, 6th IEEE International Conference on Industrial Informatics, 973-978, available at: <https://ieeexplore.ieee.org/document/4618243>
- Kastner, W. (2016), “KNX goes IoT – Aufbruch ins IoT mittels KNX - Webservices”, 7. ZVEI Kolloquium Gebäudeautomation Fachverband Elektroinstallationssysteme, available at: <http://hdl.handle.net/20.500.12708/86388>
- Kayas, G., Hossain, M., Payton, J. and Islam, R. (2020a), “SUPnP: secure access and service registration for UPnP-enabled internet of things”, *IEEE Internet of Things Journal*, Vol. 8 No. 14, pp. 11561-11580. available at: <https://ieeexplore.ieee.org/document/9352973>

-
- Kayas, G., Hossain, M., Payton, J. and Islam, R. (2020b), "An overview of UPnP-based IoT security: threats, vulnerabilities, and prospective solutions", 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 452-460, available at: <https://ieeexplore.ieee.org/document/9284885>
- Koch, S., Davis, S., Lobb, N., Marchionini, M., May, M. and Williams, G. (2019), "CAFM systems", in Williams, G. and May, M. (Eds), *The Facility Manager's Guide to Information Technology*, IFMA, pp. 271-316.
- Kost, E. (2024), "What is UPnP? Yes, it's still dangerous in 2024", available at: www.upguard.com/blog/what-is-upnp
- May, M. and Williams, G. (Eds) (2017), *The Facility Manager's Guide to Information Technology – An International Collaboration (2nd Edition, 635)*, IFMA.
- Miller, K. and Van der Beek, W. (2014), "UPnP. Internet of things", UPnP Forum, available at: https://upnp.org/resources/documents/UPnP_IoT_Overview_Dec2014.pdf
- OCF (2024), "UPnP standards and architecture", available at: <https://openconnectivity.org/developer/specifications/upnp-resources/upnp>
- Redlein, A. and Höhenberger, C. (2020), "Digitalisation", in Redlein, A. (Ed.), *Modern Facility and Workplace Management: Processes, Implementation and Digitalisation*, p. 147. Springer.
- Ritter, T., May, M. and Schlundt, M. (2019), "CAFM trends and outlook", in Williams, G. and May, M. (Eds), *The Facility Manager's Guide to Information Technology*, pp. 399-410. IFMA.
- Schuster, B., Aßmann, U., Korzetz, M. and Kühn, R. (2018), *Smart Rooms – Effizienter Betrieb Von Gebäuden Durch IoT*, INservFM Kongress, pp. 231-240.

Corresponding author

Asbjörn Gärtner can be contacted at: asbjorn.gaertner@rptu.de