Ontology-based Model for Trusted Critical Site Supervision in FUSE-IT

Shohreh Ahvar*, Gabriel Santos†, Nouredine Tamani‡, Bernard Istasse§,
Isabel Praça†, Paul-Emmanuel Brun¶, Yacine Ghamri‡, and Noël Crespi*
*Telecom SudParis, Evry, France; ¶Airbus Defence & Space, Paris, France †GECAD, ISEP/IPP, Porto, Portugal
‡University of La Rochelle, La Rochelle, France, §EISIS/Arc Informatique, Nantes/Paris, France
*{shohreh.ahvar, noel.crespi}@telecom-sudparis.eu; †{gajls, icp}@isep.ipp.pt
‡{nouredine.tamani, yacine.ghamri}@univ-lr.fr, §bernard.istasse@neuf.fr, ¶paul-emmanuel.brun@airbus.com

Abstract—**Smart buildings combine ICT and IoT technologies (e.g., smart appliances, sensors, actuators and smart meters) in order to provide supervision functions for Building Management Systems (BMS), which are capable to monitor and control both their physical elements (e.g., energy systems, network and storage facilities) and conceptual elements (e.g., building users, usage scenarios, security and trust and intrusion). To develop such systems, there is a need for a common information base which is expressive and flexible enough to describe building elements, their characteristics and interrelationships, as well as the constraints that apply to them. Despite the plethora of existing BMS models, there is still a lack of a common model showing a large compatibility and interoperability with existing BMS. Therefore, we introduce in this paper FUSE-IT ontology which provides a unified view of smart buildings by merging IoT/BMS ontologies such as Semantic Sensor Network (SSN), Smart Appliances REFerence (SAREF), Smart Energy Aware Systems (SEAS), among others. The obtained model is the basis of smart BMS we are aimed to implement within the FUSE-IT project to ensure global physical and cyber security, trust and safety in critical sites.**

I. Introduction

Building Management System (BMS) is a core-corner component in any smart buildings. It concentrates all information and decisions to be made to ensure the good and secure functioning of their cyber and physical elements. It is even crucial when it comes to critical sites where a large amount of sensors, actuators, smart appliances, smart meters, and many other IoT objects are deployed and used to collect data about diverse aspects of a building such as presence, lighting, temperature, to name a few. Having a sustainable, reliable, user-friendly, efficient, safe and secure BMS is thus becoming a major challenge. Within the framework of FUSE-IT project (www.itea2-fuse-it.com), such a process encompassing *cross-domain KPIs* is the core component of the Smart BMS [1], which targets the evaluation of the *four activity domains* a critical site administrator aims to supervise, namely: Energy supply and efficiency (e.g., micro-grids, energy monitoring, storage), Facility and building automation (e.g., heating, ventilation and air conditioning, lighting), Information and Communication (e.g., local area networks, indoor wireless), and Security and safety (e.g., fire detection, anti-intrusion video-surveillance).

These domains need to be described within a unified data model, in order to empower buildings with strong security and safety functions, since critical sites are constantly under the threat of security violations, either on their physical or on their IT infrastructures. Moreover, threats can be originated from any of these domains at the same time. Facing the huge number of sensors and their heterogeneity, traditional data modelling, storage and processing methods, such as relational databases and related technologies, are unfortunately not capable to deal with such complex data. Furthermore, the process of decision making in such contexts needs to go beyond the classical query/retrieval schema to handle more sophisticated ways to analyse an event such as deductive and inductive reasonings, and efficient data interlinking in order to extract significant information for safety, security and trust management within critical buildings. To do so, it is important to shift the data model to a new and a more adapted model based on logics such as description logics and their related well-known data structure called ontologies.

Therefore, we introduce in this paper the ontological model we developed in FUSE-IT project for smart BMS, which describes a Unified View (UV) of the concepts and data involved in the above mentioned domains. It merges different ontologies already developed in each domain such as Semantic Sensor Network (SSN) [2], Smart Appliances REFerence (SAREF) [3], Smart Energy Aware Systems (SEAS) [4] ontologies, etc. The aim of the obtained model is to provide a generic and an overall view of smart buildings, covering necessary concepts and relations to ensure safety, security, and trust within critical sites. Such a global view model can be seen as a first attempt to build a unified data model for smart buildings to encompass their main aspects, which are actually not or only partially covered in existing BMS ontological data models [5].

Section II summarizes some related work in the field of BMS data models. Section III recalls FUSE-IT building management framework. Section IV describes the main elements of the FUSE-IT BMS ontological data model, and Section V concludes the paper.

This work was partially funded by the ITEA 2 FUSE-IT project “Facility Using Smart secured Energy and Information Technology”.

978-1-5090-3672-1/17/$31.00 ©2017 IEEE

II. Related Work

Many projects are elaborating semantic models for facilitating the management of buildings by focusing on a specific single aspect of a building. From metadata development point of view, Haystack [6] and Brick [7] projects are aimed at bringing intelligence on building equipments and developing strong metadata models that should help implement realistic cases of building description with applications for demand response, fault diagnosis, occupancy model, etc [7]. Despite the announcement of these possibilities for such applications, the ontology developed so far is more a taxonomy and seems currently lacking the potential of actionable entities with a weak development of relationships between concepts. The case of event management is not treated by the project Brick while in previous initiatives led by IBM on similar metadata their project has led to including SSN ontology with additional inclusion of modular ontologies (physical process and smart building) [8].

Considering actionable entities, the reference that brings consensus from a large panel of organizations is the base ontology from OneM2M [9]. Efforts are ongoing at the European Telecommunications Standards Institute (ETSI) with the extension towards the case of smart appliances controllable as plug loads. The initiative has brought to the definition of SAREF, an ontology that is dedicated for smart appliances control of their energy consumption, control devices (meter, switch, sensor), and actionable command and services through strong relationships. This ontology acts as a pivot ontology with other ontologies such as SSN, which is an important component for several initiatives in the context of IoT. The initiative is being extended to include building reference component with the alignment with Industry Foundation Class (IFC) [10] on the one hand, and energy control and demand response capabilities, with the support of EEBus and Energy@Home projects [11], [12], on the other hand.

Besides, there are some developments of modular ontologies for Smart Buildings and related needs within SEAS project in the context of Smart Grid. However, these ontologies are kept at the level of taxonomies.

Another significant work for facilities and assets description has been developed under the responsibility of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) [13]. As a result, Facility Smart Grid Information Model (FSGIM) [14] can be used as an Uniform Model Language (UML) and translated into an ontology format. One of its interests is the support of electrical energy consumer participations in smart grid networks.

Given all the aforementioned models, they are still not adequate for the problem at hand, since their model takes into account only a subset of building aspects. Therefore, they are not sufficient to consider the case of Critical Sites, where FUSE-IT is dealing with four key domains (Energy, Security, Facility, and ICT). In addition, neither ICT nor security are well covered. Therefore, project is building a reference model based on gathering several ontologies among the ones described above, with in particular the adjunction of security ontologies like Intrusion Detection System ontology (IDS) [15], security credentials and access. Moreover, it is note worthy that there is a lack in describing metadata and making data actionable in interoperable context of systems, which are interconnected and protected by secured services, which is one of challenging goals of FUSE-IT.

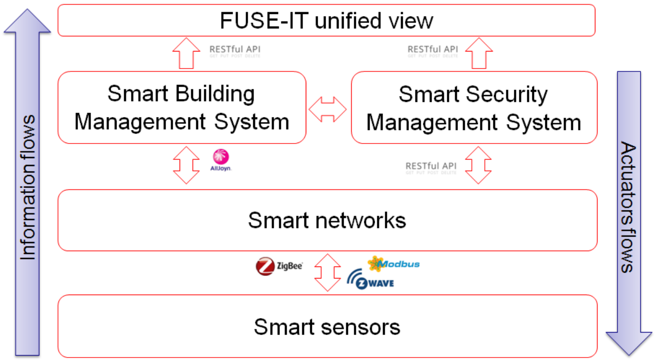

Fig. 1. FUSE-IT building management framework

III. FUSE-IT System Architecture

FUSE-IT fosters innovations by synergies between all four activity domains on four System Layers: 1) Smart sensors, effectors and actuators, for cross domain and secure data acquisition and control, 2) Smart Energy and Information networks, seeking the best combination/federation of network technologies and proposing optimized architectures for corporate networks combining energy efficiency, flexibility, security, reliability and open protocols, 3) Smart Building Management System (SBMS), for the intelligent and timely management and control of building resources, 4) Smart Security Management System (SSMS), for corporate networks and microgrid security, improved identity and access management, as well as data integrity and user authentication, enhanced virtual networks and segregation capabilities.

At management level FUSE-IT fosters a SBMS adapted to critical sites with a core Building Data Processing and Analysis module, Smart Secured Remote Management solutions, improved Human-Machine Interfaces and Innovative Service Offering. The core of SSMS is to achieve a Protected Building through the integration of System Security, Network Security and Building Security. The UV provides a holistic view of the building for ease of use. It is built on the top of the SBMS and SSMS interfaces, all the 3 with a unique authentication mechanism. High-level information is displayed in the UV such as cross-domain indicators, or alarm synthesis and high level/critical alarms. From a given item, it will be possible to get further details in SBMS or SSMS interfaces. Fig. 1 illustrates FUSE-IT approach and high level system design.

IV. Ontological model

As previously stated in the introduction, the FUSE-IT project combines *four activity domains*. Accordingly, the ontological model developed gathers concepts and relationships from different ontologies related with the distinct domains.

When developing ontologies, it is a major requirement to reuse, as much as possible, publicly available ontologies of the covered domains. The FUSE-IT ontology is built upon some existing ontologies, namely the SSN, SAREF , SEAS , IFC4 [16], Ontology Web Language for web Services (OWL-S) [17], IDS, and the Unified Cybersecurity Ontology (UCO) [18]. Some of these heterogeneous ontologies share concepts with the same meaning, such as *seas:Device* and *saref:Device*, leading to the need of ontology alignment to determine the correspondences between concepts and/or relations in the different ontologies. Integrating, this way, data from heterogeneous sources while helping heterogeneous systems to interoperate.

Each domain is modeled using a set of concepts and relationships gathered from the various ontologies. For the *Energy and Smart Grids* domain where considered concepts and relations from SEAS and SAREF. SEAS knowledge model is a modularized and versioned ontology enabling interactions between consumption and production energy systems in a smart grid in order to optimize global energy use. In turn, SAREF ontology is a shared model aiming at easing the matching of existing assets in the smart appliances domain, providing building blocks that enable the separation and recombination of distinct parts of the ontology, given the specific needs. Ontologies alignments were made to ensure the correct correspondance between concepts and/or relations with the same meaning.

The *Building Facilities* domain includes concepts and relations from SEAS, SAREF and IFC4 ontologies. IFC is an open specification for Building Information Modeling (BIM) data shared/exchanged in a building construction or facility management project. It represents the international openBIM standard. Likewise, an ontology alignment was performed to map related concepts/relationships.

The *Security* domain model is covered by the SSN, OWL-S, IDS and UCO ontologies. SSN is able to describe sensors, their capabilities and accuracy, their observations and methods used to sense. OWL-S describes properties and capabilities of Web services in unambiguous, computer-interpretable form. From it, only the modules *Credential Ontology* and *Privacy Ontology* have been added. The former provides classes on security mechanisms for authentication purposes, which may be associated with assets/sensors to ensure the level of security needed. The latter, expresses privacy policies and the setting of rules to be applied between the client and the service. The IDS ontology models computer attacks and it is used to ease the reasoning process of detecting and mitigating computer intrusions. In turn, UCO, an extension of the IDS, supports information integration and cyber situational awareness in cybersecurity systems.

Finally, the *ICT* domain model is composed of all the ontologies mentioned above. Fig. 2 illustrates the FUSE-IT knowledge model considering its four domains and the ontologies included in each one.

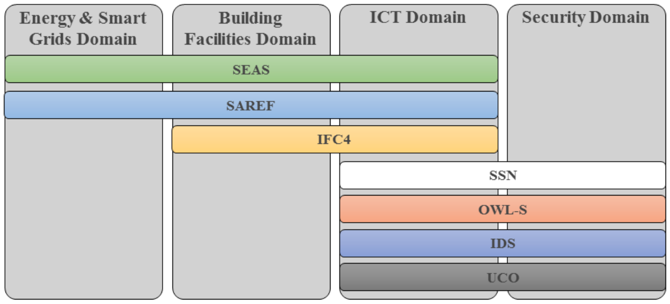

Fig. 2. FUSE-IT domains & respective knowledge model

V. Conclusion

This paper positioned the definition and exploitation of FUSE-IT ontology as an unified data model for the FUSE-IT Building Management System architecture developed for the next-generation of BMS for Critical Sites. FUSE-IT ontology gathers well-identified concepts and relationships from different ontologies dealing with four key domains (Energy, Security, Facility, and ICT) which are not (or only partially) covered in existing BMS models.

As future work, the proposed BMS ontological model will be instantiated within an ongoing prototype for the final demonstrator of FUSE-IT project.

References

[1] H. Pouyllau, B. Istasse, S. Ahvar, N. Crespi, I. Praa, S. Garcia Rodriguez, and E. Mengusoglu, “Fuse-it: Enhancing critical site supervision with cross-domain key performance indicators,” in *Global Information Infrastructure Symposium*, 2016.

[2] “”ssn ontology”,” https://www.w3.org/TR/vocab-ssn/.

[3] “Saref ontology,” http://ontology.tno.nl/saref/.

[4] “Seas ontology,” https://w3id.org/seas/ .

[5] B. Balaji, A. Bhattacharya, G. Fierro, J. Gao, J. Gluck, D. Hong, A. Johansen, J. Koh, J. Ploennigs, Y. Agarwal *et al.*, “Brick: Towards a unified metadata schema for buildings,” in *Proceedings of the ACM International Conference on Embedded Systems for Energy-Efficient Built Environments (BuildSys). ACM*, 2016.

[6] “Haystack project,” http://project-haystack.org/ .

[7] “Brick schema,” http://brickschema.org/.

[8] A. S. J. Ploennigs and F. Lecue, “Adapting semantic sensor networks for smart building diagnosis,” in *International Semantic Web Conference*, 2014, p. 308 323.

[9] “Onem2m ontology,” http://www.onem2m.org/technical/developers-corner/tools/onem2m-ontologies/.

[10] “Buildingsmart,” http://buildingsmart.org/ifc/ .

[11] “Energy-home,” http://www.energy-home.it/SitePages/Home.aspx.

[12] “Eebus,” https://www.eebus.org/en/about-us/.

[13] “Ashrae,” https://www.ashrae.org/ .

[14] “Fsgim ashrae standard project committee 201 (spc 201) facility smart grid information model,,” http://spc201.ashraepcs.org/.

[15] A. J. J. Undercofer, J. Pinkston and T. Finin, “A target-centric ontology for intrusion detection,” in *18th International Joint Conference on Artificial Intelligence*, 2004, pp. 9–15.

[16] “Ifc,” http://www.buildingsmart-tech.org/specifications/ ifc-releases/ifc4-release.

[17] “Owl for services (owl-s),” http://www.ai.sri.com/daml/services/owl-s/ .

[18] Z. Syed, A. Padia, M. L. Mathews, T. Finin, and A. Joshi, “UCO: A Unified Cybersecurity Ontology,” in *Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security*. AAAI Press, February 2016.