# Device Description in HYDRA Middleware

Martin SARNOVSKÝ[1,2], Peter KOSTELNÍK[2], Ján HREŇO[2], Peter BUTKA[1,2]

[1] Faculty of Electrical Engineering and Informatics, Technical University Košice
Letná 9, 040 01 Košice, Slovak Republic,
{martin.sarnovsky, peter.butka}@tuke.sk
[2] Faculty of Economics, Technical University of Košice, B. Nemcovej 32, 040 01
Košice, Slovak Republic,
{peter.kostelnik, jan.hreno}@tuke.sk

**Abstract.** This paper describes semantic-based device description which will be designed and implemented in the IST-2005-034891 project HYDRA ("Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture") funded within the FP6 IST Programme. HYDRA project aims at development of middleware for intelligent networked embedded system based on service-oriented architecture, deployable on both new and existing networks of distributed wireless and wired devices. The embedded service-oriented architecture will provide interoperable access to data, information and knowledge across heterogeneous platforms. These devices and their local networks will also be interconnected through broadband and/or wireless networks. An implemented HYDRA middleware and a toolkit will be validated in real end-user scenarios in three different user domains: Facility management (smart/intelligent homes), Healthcare, and Agriculture. One of the most important aspects of middleware design and implementation is usage of semantic device descriptions for different purposes. In this article we will focus on semantic description of devices and their capabilities using device ontology.

**Keywords:** networked embedded systems middleware, semantic technology, ontology modelling, semantic security, device ontology

## 1. Introduction

The HYDRA project is addressing the problem, which is frequently faced by producers of devices and components - the need for (which is actually becoming a trend) networking the products available on the market in order to provide higher value-added solutions for their customers [3]. This requirement is implied by citizen centred demands requiring intelligent solutions, where the complexity is hidden behind user-friendly interfaces to promote inclusion. The vision of the HYDRA project is ambitious*:*

*"To create the most widely deployed middleware for intelligent networked embedded systems that will allow producers to develop cost-effective and innovative embedded applications for new and already existing devices."*

To put it in practical terms: In the ambient world of the near future, interconnected intelligent devices will surround us, at home, work, or while travelling. These devices and their local networks will also be connected to the outside world through broadband and/or wireless networks [2]. Numerous services to support us in our personal life will be provided through these ambient devices and over the connection to the outside world. To adapt to our personal lifestyle, and to offer the right service at the right time in the right place, such services will rely on the use of private data - which means putting emphasis also on security and privacy. It is expected that the HYDRA will contribute to this scenario.

HYDRA will develop a middleware based on a Service-oriented Architecture (SOA), to which the underlying communication layer is transparent. Hydra middleware will be designed to run on a variety of stationary and mobile devices. The middleware will include support for distributed as well as centralised architectures, security and trust, reflective properties and model-driven development of applications. It will be deployable on both new and existing networks of distributed wireless and wired devices, which operate with limited resources in terms of computing power, energy and memory usage. It will allow for secure, trustworthy, and fault tolerant applications through the use of novel distributed security and social trust components and advanced Grid technologies.

The embedded and mobile Service-oriented Architecture will provide interoperable access to data, information and knowledge across heterogeneous platforms, including web services, and support true ambient intelligence for ubiquitous networked devices. Furthermore HYDRA will develop a Software Development Kit (SDK), which will be used by developers to develop innovative Model-Driven applications using the Hydra middleware. Middleware and connected devices should enable developers to implement applications that depend on and adapt to context information. In particular, the developers stressed the acquisition and management of spatial context information that allows for locating devices attached to the system and for the positioning of people and assets. The HYDRA project will validate the middleware, the SDK toolkit in real end-user scenarios in three user domains.

## 2. Device Ontology

One of the key components in the Hydra middleware is the Device Ontology, where all meta-information and knowledge about devices and device types are stored. Our Device Ontology is based on the FIPA Device Ontology [4], which specifies a frame-based structure to describe devices, and is intended to facilitate agent communication for purposes such as content adaptation. Device description contains basic information related to a device such as the device name, vendor details, hardware description and software description used to describe hardware and software resources of the device. The purpose of the Application Ontology Manager is to provide an interface for using the Device Ontology. This manager could possibly also maintain other models in addition to devices.

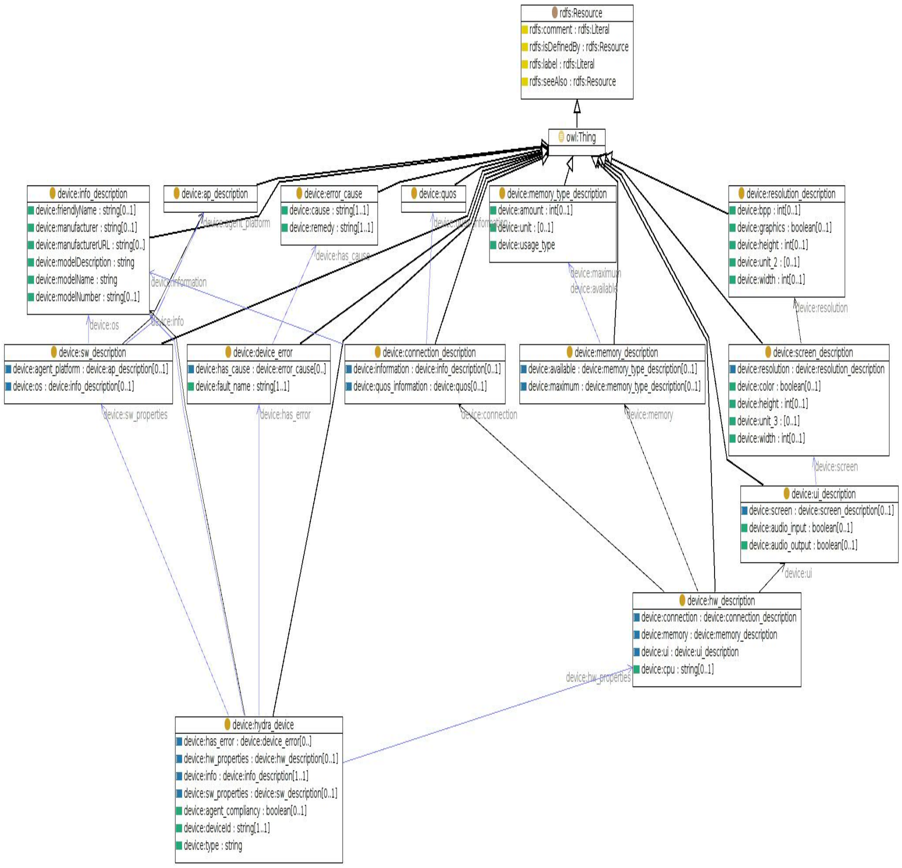


**Fig. 1.** Device Ontology in HYDRA

The semantic description will, in a general way, define the capabilities of the devices and the security requirements of the device. This is necessary in order to support interoperability among heterogeneous and distributed Hydra-enabled devices, but it also facilitates the task of virtualisation. The semantic description should allow individual devices to specify the type and level of security services that they both require and provide. This allows Hydra to match devices that may operate in concert, i.e., where the security requirements of all the devices are satisfied, and to reason about the overall level of security achieved by the aggregation of these devices. For example, messages delivered through different devices (e.g., in multi hop-/mesh networks) will be forwarded by devices that provide different levels of security, so it is important to be able to determine the minimum level of security offered by these devices. Without knowing the security services provided by the different devices, it will be impossible to reason about the overall security that can be guaranteed for such communication. Semantic parameterisation of devices according to their capabilities and their associated security domains will help in finding an optimum solution to these types of situations and hence it is vital to Hydra that we define a clear semantic framework representation for interoperability of devices to support secure, trusted services. This is essential for heterogeneous device networks where devices might exist which have very few features in common.

## 4. Conclusions

The device ontology is considered as one of the model components in the Hydra. This ontology with related semantic services will be used both in design- and in run-time. At design time (by users of the IDE/SDK) by allowing developers to query on device properties and functions, in run-time the ontology will be used by the various services for device management (discovery, updates etc.).

We foresee that a basic ontology support is part of the generic Hydra platform, with extension possibilities given to developers. A user (of the IDE/SDK) in the future should be able to manually update device ontology. The system should also provide a certain level of automated updates, by generating and updating ontology contents from device/product documentations. Similarly, detection of modifications made to a device (e.g., a vendor software upgrade) should be possible and result in updates of corresponding ontology elements.

**Acknowledgements**. The work presented in the paper is supported by the EC within the FP6 IST-2005-034891 Project "HYDRA - Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture".

## References

1. Hydra: D2.1 Scenarios for usage of HYDRA in 3 different domains. Hydra Project Deliverable, IST project 2005-034891, 2006.
2. Hydra: D2.5 Initial Requirements Report. Hydra Project Deliverable, IST project 2005-034891, 2006.
3. SARNOVSKY, M., BUTKA, P., KOSTELNIK, P., LACKOVA, D.: HYDRA – Network Embedded System Middleware for Ambient Intelligent Devices, In: ICCC'2007: Proceedings of 8th International Carpathian Control Conference, Štrbské Pleso, Slovak Republic, May 24-27, pp. 611-614, 2007.
4. FIPA. FIPA Specifications. http://www.fipa.org/specs/fipa00091/