# OPC UA based Smart Home

# Abstract

Object Linking and Embedding for Process Control Unified Architecture, knows as OPC UA is the most recent released industry standard from OPC Foundation, which compared with his predecessors is equipped with a list of charming new features, with whose help OPC UA is capable of solving imperfections that come along with OPC and offering more functionalities to the end users. In this paper, I will describe highlighting features of OPC Unified Architecture, especially focus on the security issues, analyze already well known attacks and corresponding countermeasures taken by OPC Unified Architecture, evaluate performance of different possible security polices and design a OPC UA standard based Smart Home to illustrate the implementation of essential parts of OPC Unified Architecture.

# Introduction

OPC from OPC Foundation has already found a great application area in today’s industry world, providing a set of standards used to support system interconnectivity and realize a common interface for communications between different products from different vendors. According to OPC Unified Architecture the future standard for communication and information modelling in automation from Wolfgang Mahnke, Stefan Leitner, there are over 22,000 products applying OPC offered by 3,200 vendors in automation industry.[1]

Even OPC standards are widely accepted, there exit still limitations. I.e. Most of all, OPC is windows platform dependent and based on Microsoft COM/DCOM technology, which is already deemphasized and shows less attraction compared with platform independent Web Services. Moreover although COM/DCOM should help OPC to conquer cross-computer distribution weakness, but it also brings several drawbacks. For instance, developer is not capable of controlling DCOM and has to face frequent DCOM configuration issues. [wiki] Also OPC only supports simple date type information and provides single hierarchy, which apparently is not able to meet increasing need from users. [2] And etc.

In order to solve all these imperfections, OPC Unified Architecture comes into the world, which is a radical update of OPC protocols and aimed to achieve simplicity, scalability, outstanding performance, perfect and flexible security, cross platform, always availability, robustness ,supporting complex date types.

In conclusion, OPC Unified Architecture is a platform independent industry policy, supports the secure communication based on different network conditions between client and server that are provided by various vendors.

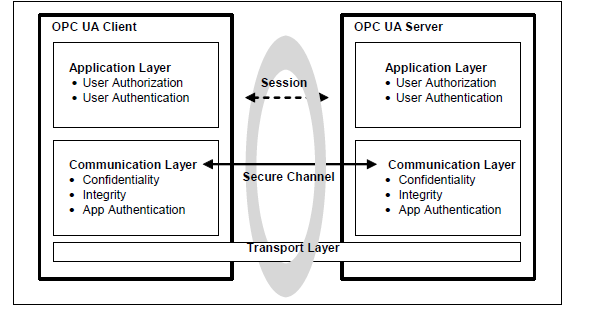
# OPC Unified Architecture Structure Overview

The whole OPC Unified Architecture specification is divided into three main parts, core specification parts, which consists of OPC UA concepts, security model, address space model, services, information model, service mapping and profiles, access type specification parts including date access, alarm and conditions, programs and historical access, at last utility specification parts covering discovery together with aggregates.

In OPC Unified Architecture information that can be visited by clients is defined as address space [Spe1]and there is a set of services provided by OPC UA which are introduced in order to apply operations in the address space. The information in address space is organized as a set of in particular hierarchy structured objects. Clients can accept information provided by OPC Unified Architecture Servers in two major ways, binary structured data and XML documents, depending on the complexity of exchanged information, network quality and so on. In addition three kinds of transport protocol can be applied to support client server communication. They are: OPC UA TCP, HTTP/SOAP and HTTP. Also the hierarchy structure in which objects are organized in address space is also various according to OPC UA standards and not limited to simple single hierarchy.

Another charming feature of OPC UA is Event Notifications. With the help of Event Notification, OPC UA servers are allowed to immediately after some conditions are satisfied publish data, which is subscribed by clients. In this way, clients can for instance discovery failures within client-server-communication quickly and recover as soon as possible, which in return minimizes the lost to the smallest possible amount and also they are able to observe the subscribed data more precisely and find the pink elephant as fast as possible.

Since some data exchanged between client and server could be extreme precious and should be protected from other malicious third party, OPC UA defines a full set of security model, with which developer of system can configure the security level of the application to meet the need of reality. With the security model, authentication of client and server, authorization, integrity and confidentiality of client-server- communication, auditability and availability of services are guaranteed. Also OPC UA provides a set of countermeasures against message flooding, eavesdropping, message spoofing message alteration, message reply, server profiling, session hijacking and so on[Spe2].



Above [Spe4] is the typical security architecture of OPC UA. As shown in 1, the communication between OPC UA client and server is established above a secure channel, which is active during the whole application session. The secure channel is established only after successful validation of both client and server certificates. This secure channel provides necessary mechanisms to support confidentiality, message integrity and application authentication. On top of secure channel, is an application level session between OPC UA client and server, whose responsibilities are to transmit data information and commands. This session is also in charge of managing security policies like user authorization and authentication. It should be pointed out that, even a secure channel is out of work for some reasons, the session is still valid and OPC UA client and server involved in aforementioned session can still re-establish the broken secure channel. A secure transport layer is guaranteed by encryption and signatures defined by platform that support web services.

Last but not least security feature offered by OPC Unified Architecture is auditing, which supports traceability of any behaviours occur in OPC UA system. That means any security related problem can be recorded and for future use.

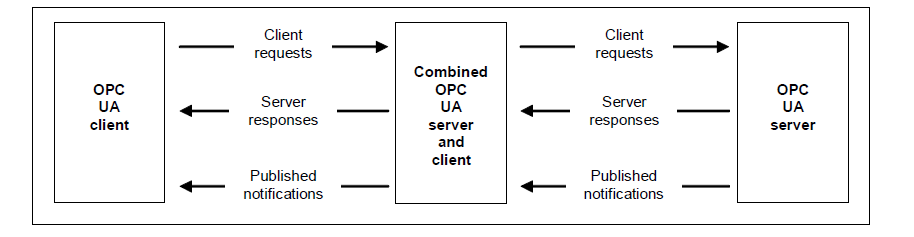


Figure 2 illustrates a typical OPC UA client server architecture and also describes a combined server-client. The routine communication between client and server consists of request from client, corresponding responses sent from server and notifications which are generated because of client’s early subscription.

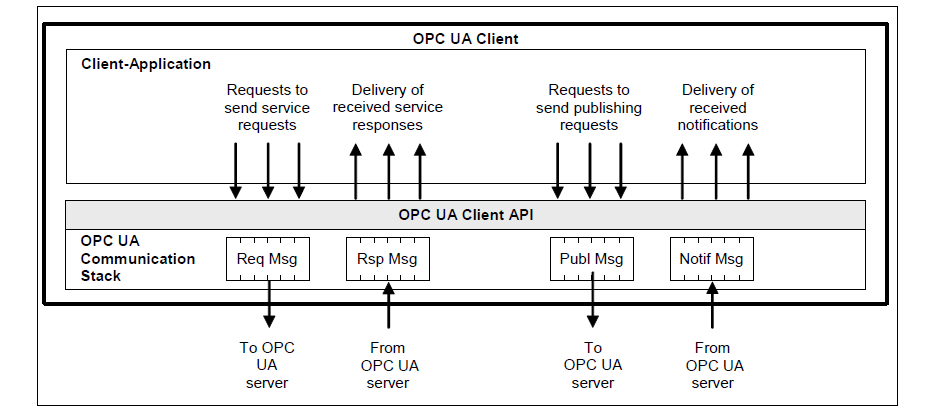
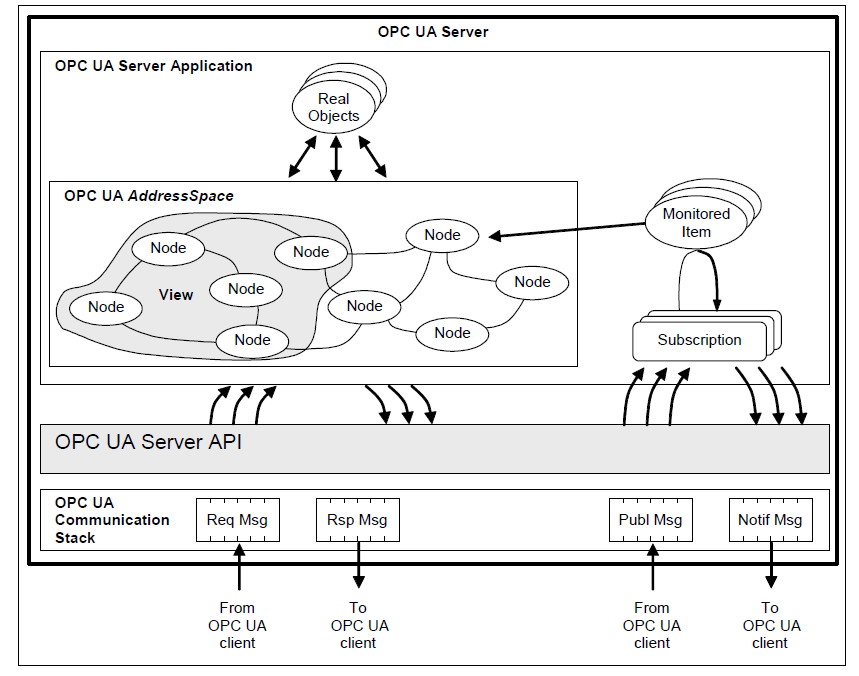


Figure 3 picture one simple OPC UA client containing client application, an internal API, isolating the application code from communication stack , and a communication stack that translates OPC UA client API calls.



In figure 4, one OPC UA Server structure is explained. As the aforementioned client structure, it also includes three main parts, server application, internal API and communication stack. It is worth mentioning that, real objects here are referred as physical field devices or software application that is only maintained internally. View, which is pictured as a part of address space, presents nodes that can be browsed by clients.

# Implementation Scenario

# Time Lines

1 OPC UA – Service-oriented Architecture for Industrial Applications

Stefan-Helmut Leitner, Wolfgang Mahnke

2 OPC UA – Service-oriented Architecture for Industrial Applications

Stefan-Helmut Leitner, Wolfgang Mahnke

3 OPC UA specification 1-11(old)

4 OPC UA – Service-oriented Architecture for Industrial Applications

Stefan-Helmut Leitner, Wolfgang Mahnke

5 Implementation of the OPC UA Information Model for Analyzers

Version 1.00

*Mariusz Postol (CAS), Voytek J. Janisz (ABB), Claude M Lafond (ABB), Jim Luth (OPC Foundation)*