Executive Summary

February 2009 marked the final release of the OPC Unified Architecture (UA) Phase One Deliverables. The more people hear about OPC UA, the more questions that seem to arise. What exactly is OPC UA and what does it mean to me? When will products be ready? Can my people implement it and should they be doing it now? Not to mention questions about security, scalability and backwards compatibility.

OPC UA covers a wide range of topics and functionality, but what people really want to know is: What is it, how does it help me, and where can I get it? These questions are best summed up in the five things everyone needs to know about OPC UA.
#1 - Service Based Solutions for Today and Tomorrow

The OPC Unified Architecture (OPC UA) is a set of specifications that standardizes industrial connectivity. OPC UA is the unification and next evolution of the classic OPC specifications that have provided interoperability for industrial automation for the last ten years. OPC-UA is described in a layered set of specifications broken into multiple Parts. The core specifications are purposely described in abstract terms. The implementation parts map the standards to existing technology on which software can be built. This layering is by design and helps isolate the OPC UA specifications from the inevitable changes in the technology used to implement it. OPC UA is based on Service Oriented Architecture (SOA). SOA is an architectural style whose goal is to achieve loose coupling among interacting software agents. A service is work done by a service provider to achieve desired results for a service consumer. In other words services represent abstraction actions the OPC UA server can perform at the OPC UA client’s request.

The idea of SOA departs significantly from object oriented programming, which encourages programmers to bind data and its processing together. The classic OPC specifications were closely tied to Microsoft’s object oriented COM and DCOM technology. While the classic OPC specifications allowed programmers to quickly understand how interfaces would be implemented, the close coupling came at the cost of flexibility, extensibility and longevity of the interfaces. OPC UA is designed to not only provide solutions for today’s implementations, but to be adaptable and extensible for the years to come. By following the rules of service oriented architectures, OPC UA solutions will remain unchanged at the application level even when the underlying technology changes in the future.

OPC UA is based on the following guiding principles for service based architectures:

- First, have a relatively small set of simple interfaces to all participating software applications. Since there are only a few generic interfaces, the application-specific semantics are described in messages. The services are defined by the Core Specification Parts which ensure interoperability among applications. Application specific messages are defined in other Parts which allows for flexibility.

- Second, the messages are written in a format, structure, and vocabulary that is understood by all OPC UA applications. Limiting the vocabulary and structure of messages is a necessity for any efficient communication. The more restricted a message is, the easier it is to understand the message, although it comes at the expense of reduced extensibility.

- Third, extensibility is vitally important. Industrial environments are an ever-changing place. Those changes demand corresponding changes in the OPC UA software system, service consumers, providers, and the messages they exchange. If messages are not extensible, users would be locked into one particular version of a service. Restriction and extensibility are deeply entwined, but both are needed and increasing one comes at the expense of reducing the other. The OPC UA specifications strive to have the right balance of both and Compliance testing to ensure they are implemented properly.
Of course another feature is that Service-based architecture is internet and fire-wall friendly, they will avoid the issues associated with DCOM. However, while the limitations of Microsoft DCOM are a big challenge for existing classic OPC implementations, building OPC UA on service-based technologies offers many other advantages. OPC UA is the next generation in industrial connectivity for the entire enterprise which incorporates and extends all existing OPC functionality.

#2 - Security To Fit Every Need

OPC UA provides the infrastructure to provide multiple tiers of security implementation. OPC UA Security consists of authentication and authorization, encryption and data integrity via digital X.509 certificates. X.509 is a standard for PKI (Public Key Infrastructure) in cryptography, which defines specific formats for PKC (Public Key Certificates) and the algorithm that verifies a given certificate path is valid under a give PKI. Putting the security jargon aside, it is suffice to say OPC UA security is built on accepted Internet and Service security practices.

OPC UA servers from different vendors will provide different tiers of security which balance security versus convenience. The OPC UA specifications provide a consistent foundation that allows vendors to develop applications that meet any tier’s requirements without having to re-architect the application. This foundation also allows users to choose a lower tier if that is all their application requires.

- **Small Ad-hoc Network Tier** - The OPC UA client applications would be issued a self-signed certificate. The OPC network administrator would manually add the certificates to a trust list the OPC UA server references. Only OPC UA applications in the trust list would be granted access. This installation step would be much simpler than the DCOM configuration process of classic OPC implementations today.

- **Normal Corporate Network Tier** - Trust in some systems is based on some outside source. This is the role of an external Certification Authority. The OPC UA application would be issued certifications which are issued by a company controlled or corporate Certification Authority. At installation time, each OPC UA application would be issued the certificate and be configured to trust all certificates from the company CA.

- **High Security Tier** - In the High Security tier OPC applications would use a combination of local trust lists and Certification Authorities. Each application’s trust list would have to be managed centrally but administrators would have fine grain control over who as access to what. OPC Security Gateway servers could be used to provide access to other Servers using lower security tiers, or to provide users with easy management of security settings.

- **Anonymous Web Client Tier** – In the final tier the OPC UA application would ensure privacy and integrity by authenticating using username/passwords after a secure connection is created. After proper authentication, each application would be issued a certificate with a Private key, but no advance trust relationship is required.

OPC UA is flexible enough to meet any implementation need, yet be secure. Security is built into the core of the OPC UA specifications, so products are ‘secure-by-default’. Vendors must specifically turn off security if that is what a particular customer or scenario needs.

“MatrikonOPC continues to be the leader in industrial connectivity. By adding UA functionality to their Security Gateway, they are not only demonstrating their commitment to OPC Unified Architecture, but they are also providing end users with natural point to start integrating OPC UA into their existing architectures,” Says Tom Burke, President of the OPC Foundation.
Existing OPC implementations typically deal with the challenges DCOM and Security by employing OPC Tunneling solutions, such as the MatrikonOPC Tunneller. These provide the functionality and interoperability of the OPC specifications while using ‘internet friendly’ transportation mechanisms.

#3 - More than Microsoft

The business problems facing IT organizations today have not changed, they just got bigger. Corporate pressure for better utilization, integration of historically separate systems and faster implementation of new systems is constant, while environments are growing more complex. Tightening budgets demand legacy systems be reused rather than replaced. At the same time organizations are merging or companies are being acquired meaning more disparate systems need to be integrated and absorbed. The connectivity communications must be able to accommodate an endless variety of hardware, operating systems, middleware, languages and data stores, including legacy systems and future technologies.

Since the classic OPC specifications are based on COM technology, the existing OPC installation base exists primarily on Windows. Ubiquitous Microsoft hardware at the Application and Business layers has played a major role in the wide spread adoption of OPC, however there are many control systems and applications the run on other operating systems. Also with the release of Windows Vista, Microsoft announced that while they would continue to support COM/DCOM technology well into the future, their continuing research strategy would focus on service based architectures. With these factors in mind, OPC UA has been designed to be a cross-platform solution. Having an interoperability standard that can be applied to any level of the enterprise is extremely important for building systems in today’s business world.

Existing OPC implementations typically deal with the challenges DCOM and security by employing OPC Tunneling solutions, which provide the functionality and interoperability of the OPC specifications while using ‘internet friendly’ transportation mechanisms. As these solutions are adapted to support the OPC UA specifications, they will become natural starting points for system migration. (See Figure 1) Just as these architectures provide seamless interoperability between disparate Windows systems, similar OPC UA based solutions will allow integration of Microsoft systems with embedded systems, Linux platforms or business applications based on Java.

Figure 1 – Tunnelling Options with OPC UA
It should be clear that OPC-UA does not replace existing OPC standards, but rather complements them by providing a common interoperability layer for exchanging information and a richer environment for orchestrating operations. OPC-UA embodies all the functionality of the existing OPC specifications and expands on top of them. OPC UA has maintained backward compatibility with previous standards to ensure quick adoption in the market.

As with any architecture migration of this magnitude, implementing the OPC UA specifications will be considered a challenge by many companies. The OPC Foundation has taken several steps to ensure that implementing OPC UA will be a straightforward and relatively easy process. To facilitate the adoption of the new standard and to reduce the barrier to entry, the OPC Foundation has developed an OPC UA software development kit (SDK). The SDK will be the main component developers are using to enable their existing applications or create new ones. The SDK consists of a series of application programming interfaces and sample code implementations. Since the OPC UA specification is written to be platform independent, the OPC UA deliverables provide solutions to facilitate adoption on different platforms – Microsoft .NET, ANSI C and Java implementations.

Each SDK solution is designed to fit special needs in terms of platforms, memory and processor requirements, but they are all capable to seamlessly interoperate with each other. The .NET SDK is best suited for rich, enterprise level implementations, while the ANSI C version is best suited for base implementations on embedded devices where memory and CPU utilization consideration are more important. The Java SDK implementation will be fit best with thin clients in Web environment, existing business solutions and other cross platform applications. Software vendors can choose the implementation that best fits their needs depending on requirements for performance, cross-platform capability and Internet-friendliness. Regardless of which implementation is used, the abstract service model ensures all products will be interoperable. In addition to the SDK solutions, the OPC Foundation is also providing a series of binary adapters, both client proxies and server wrappers. The adapters are used to provide direct access to all existing COM-based classic OPC clients and servers.

The OPC UA specifications, SDK toolkits, binary adaptors and other jump-start deliverables are available to all OPC Foundation members, but what about the countless thousands of classic OPC users? How and when will the advanced functionality of OPC UA be made available to them?
OPC UA is ready to go. Committed OPC vendors have been developing OPC UA products for quite some time. Now that the first phase deliverables have been field tested and approved, these products are now available in the marketplace. OPC UA covers a broad spectrum of implementations from embedded systems to full enterprise wide management systems, cross platform solutions as well as extending classic OPC installations. Therefore there are different OPC UA products available, based on what user’s need. Users who are looking to create their own OPC UA products will be members of the OPC Foundation and would take advantage of the binary adapters, various OPC UA SDK offerings and training courses available to members. However, the vast majority of OPC users around the world are those that simply want to use the technology and reap the benefits of standardized connectivity.

Classic OPC users looking to enhance their implementations with OPC UA functionality generally fall into three categories. Those who want:

1) To better unify their OPC DA, HDA and A&E products and leverage the richer information model of OPC UA.
2) A standardized way to overcome DCOM issues or deploy across other platforms.
3) Increase security in their OPC products.

Committed OPC vendors are already upgrading their OPC frameworks to support OPC UA. This provides a smooth upgrade path as more applications begin to incorporate OPC UA support, while still providing full functionality for existing classic OPC implementations. The unified service interface that OPC UA provides is a natural fit to be incorporated into OPC frameworks that already offer support for the OPC DA, HDA, A&E and Security specifications.

Since OPC UA is built on internet friendly service architecture, many users are looking to OPC UA to help with their DCOM challenges. Many of these same users currently employ some form of OPC Tunneling product to by-pass DCOM issues. Again incorporating OPC UA as the standardized transport mechanism is a natural evolution of these OPC Tunneling products. By upgrading their existing Tunneling product to an OPC UA enabled version, users can mix and match their DCOM, Tonneled and OPC UA components. This means existing classic OPC implementations do not need to change and newly added OPC UA components will communicate seamlessly as well.

OPC UA brings much to the table in terms of security, and new OPC UA products will be able to provide a wide array of security options. The easiest way for users to leverage the OPC UA security options within their classic OPC installations is by way of OPC Security Gateway products. Using an OPC Security Gateway provides item level security to existing OPC servers, plus that added certificate based security of OPC UA without having to change or modify the underlying OPC server in any way.
Now You Know

To sum things up, OPC UA can be considered the next generation in interoperability. It’s designed to extend classic OPC installations of the present and be flexible enough to prevail well into the future. OPC UA provides the functionality of current OPC and its service based architecture addresses existing shortcomings like security, platform dependence and DCOM issues. For those users who are looking to add OPC UA to their current offerings, the OPC Foundation provides its members with the documentation, tools and testing opportunities to reduce the learning curve associated with implementing the new technology. For those users who just want to know when and how they can make use of OPC UA in their existing systems, the answer is, right now by using OPC UA enabled products.

For many, embracing OPC UA will be an evolution not a revolution. Trusted OPC vendors are already providing OPC UA functionality into their classic OPC frameworks. Users can work with their vendors to determine what OPC UA functionality they need and when.

Evolve OPC systems as needed. Revel in the OPC UA functionality.

MatrikonOPC Security Gateway

MatrikonOPC Security Gateway Includes support for OPC UA! Connect multiple OPC Classic (OPC DA) servers through a single OPC security gateway and get the OPC UA connectivity you require. Security and OPC UA – an unbeatable combination.

Features and Benefits:

- Standards based security
- Access OPC servers using OPC UA, OPC Classic, or OPC Tunneller.
- Tag-level security using powerful user-based permissions combined with standard OPC security 1.0
- Works with all OPC clients who implement OPC security specifications as well as those who do not!
- Secures multiple servers at once with the ability to hide servers from unauthorized users
- Leverages existing Windows security
- Allows the user to have full control over different user access levels
- Compatible with all certified OPC DA clients and servers, regardless of vendor
About the Author

Eric Murphy, BSc, PEng, is a Chemical Engineer with a Process Control specialization and an OPC expert. Eric has been a part of the OPC community since its early beginnings. Eric is heavily involved with the OPC Foundation and currently acts as the chair for the OPC Historical Data Access (HDA) working group. Eric is also a member of the OPC Technical Advisory Council (TAC) and an active member of the OPC Unified Architecture (UA) working group. Eric has worked for companies including Honeywell and MatrikonOPC holding positions including software development architect, OPC R&D Manager, OPC Project Manager and OPC QA Manager. Eric has acted as chief consultant on hundreds of OPC projects where he has architected standards based OPC solutions.

You can often find Eric presenting online as the featured speaker for webcasts or at industry related events such as ISA Expos, OPC Conferences and other events.

For More information on OPC Architectures

For more information on OPC UA and other OPC topics be sure to follow up with these associated titles on our website at http://www.MatrikonOPC.com

Cyber Examining the Armor of OPC-UA Security
The OPC-UA specifications place key security requirements upon conformant client and server products. They also provide best-practice deployment recommendations in order to meet the anticipated security needs of users. Clearly, OPC-UA is well equipped to secure system interoperability within its realm.

OPC UA - How Deep Does Interface Standardization Go?
Prior to OPC UA, the most common complaint has been that existing OPC standards are primarily COM based. OPC UA is a service based, cross platform solution, and no longer so Microsoft centered. This issue aside, the majority of other complaints focus on the specifications not going far enough in their scope of standardization. There are criticisms that OPC does not do enough to mandate security, configuration, and providing a unified address space or defined item ‘mapping’. If you consider OPC as the standard for real time data communication, regardless of the data source, it raises an interesting question. Where does the line get crossed from a general interface specification that is open, interoperable and flexible without sacrificing usability, to one that is specialized, rigidly defined and highly integrated?