Overall Security Solutions for OPC UA Based Monitoring and Control Application

Nguyen Thi Thanh Tu(✉) and Huynh Quyet Thang

School of Information and Communication Technology,
Hanoi University of Science and Technology, Hanoi, Vietnam
tu.nguyenthithanh@hust.edu.vn,
thanghq@soict.hust.edu.vn

Abstract. Together with the global trend, the currently popular accessing model is using Service Oriented Architecture (SOA), working based on available IT infrastructure following the industrial standard OPC UA, in order to create a new environment providing monitoring, controlling and managing industrial manufacturing system effectively. In this paper, we propose a framework based on the combination between SOA and OPC UA for the designing, improving software systems applied to monitoring, controlling and managing production assembly lines. Also, we provide secuirty solution that are proposed and applied to control and monitoring system based on OPC UA standard. Basing on the proposed framework, software developers can easily implement to design, to build monitoring, controlling systems and to manage different industry assembly lines, ensuring the characteristics of inheriting developing and improving the systems flexibly, being able to enlarge and link among different systems.

Keywords: OPC UA · SOA · PKI · Webservice · Framework

1 Introduction

Opc (Object Linking and Embedding for Process Control) is an interface standard of real time computing between monitoring devices from different factories. Protocol of Dynamic Data Exchange is the solution to exchanging the first data among applications based on Windows. Technical characters of OPC based on OLE are COM and DCOM technology developed by Microsoft for operating system Microsoft Windows in family. Technical characters determine a set of standards of objectives, interface and using methods in monitoring the process and automatic applications in manufacture, which enables to interact easily. To simplify in developing device controlling software, they remove the inconsistency between controlling software, support to change the hardware character and avoid approaching conflicts in industrial controlling systems. The organization OPC defines the standard interface allows any computers to be able to get access to any OPC compatible devices. Almost all suppliers of data collecting devices and controlling devices work with the standard of OPC [1, 2]. The common specifications of OPC are: Data Access (DA), Historical Data Access

P.C. Vinh et al. (Eds.): ICCASA 2013, LNICST 128, pp. 178–187, 2014.
DOI: 10.1007/978-3-319-05939-6_18,

(HDA), Alarm and Events (A&E) and the latest is OPC Unified Architecture (OPC UA). OPC UA is being accepted in automatic industry [1, 2, 6].

Instead of using COM/DCOM technology of Microsoft, the latest standard of OPC Foundation (OPC UA) uses XML, Web services, SOA and the model of objective orient data to describe and perform three types of data: present data, historical data, alarm and events [6]. Invented in 2006, OPC UA has been attracting the interest of researchers of many universities, research centers and laboratories. Software developing companies hope that it will replace the traditional OPC successfully. OPC UA inherits all functions of traditional OPC. Moreover, OPC UA is independent of basement. It can run on Window, Linux or embedding device [7].

OPC standard is the technique which is applied widely all over the world and has obtained many great achievements in the field of industrial monitoring and controlling. A group of authors proposed to build a Framework based on new standards and techniques with high effectiveness combining between OPC UA and SOA [3–5]. In [13, 14] we introduced the development of an OPC UA SDK for both sides – OPC UA Server SDK and OPC UA Client SDK, based on the OPC UA specifications.

Recently, production processes of manufacturing companies are mostly based on IT systems. Production requests are initiated by Enterprise Resource Planning on IT systems, the execution of the process is managed by Manufacturing Execution Systems (MES), special HMIs used to for supervisory of the process, and the documentation of results, quality, and resource consumption are highly dependent on IT systems [1, 8]. OPC is an application layer for communication between software components for automation and control systems. It specially defines standardized interfaces through which OPC clients access the objects in OPC servers. With OPC foundation, they can design and implement the applications for automation and control system, but OPC DA based on COM/DCOM techniques. And DCOM security not enough to protect the industrial systems, because of this specification only providing the methods and properties which are applied to the OPC DA based COM productions. With the internet environment the security solutions proposed to use internal XML security approach for the control connection instead of the HTTP-S protocol, being described in XML Encrytion [15], XML Signature [16, 17] specifications.

Besides, OPC UA based framework for developing monitoring and control system applications using Internet environments is base of communication complying with XML, web services, and SOA. The XML signature is a system to encode digital signatures in an XML document. It uses the same standards and technologies of cryptography as usual digital signatures. The basis of digital signatures is symmetric or asymmetric cryptography. When using symmetric keys for encrypting and signing data, the same keys are used for decrypting and verifying the signature of the data, i.e., both parties in the client–server scenario have identical keys for certain cryptographic operations.

Security policy of OPC UA bases on public key infrastructure (PKI). UA defines a group of standard method sharing network that both Client and Server must install to encode data or sign on message. At each turn Client describes the method of security used. Then both Client and Server apply this method to ensure all messages to go through turn safely. There are 3 ways of security as following: None: no register, turn

off security mode. Messages can be read and counterfeited by the third party. Register: messages are signed to ensure the entire data but the body is not encoded, so they still can be read by the third party. Register and encode: register the message and encode the body can protect the data entirely.

1.1 Service Orient Architecture in Monitoring and Controlling System

Service orient architecture (SOA) is a group of rules and designing methods, developing software as the way of interactive services. These services are designed clearly, with specific functions respectively. Service plays a roll of parts of the software and can be reused depending on certain purposes [4]. The major characters of SOA are separating the communication part and service part, communication is centre of architecture. Service is approached through communication, as the way of request – respond. A service orient interaction always includes a pair of partners: Server and Client.

SOA design separates service performing with communication calling service. This creates the consistency in communication for Client application using service that is independent of what service performing technology is. Instead of building individual and massive applications, developers build sophisticated and compact services which can be implemented and reused in the whole business process. Therefore, they have outstanding distinctions such as reusability, flexibility since developers can improve the services without affecting Client using services.

Service is the key factor in SOA. It can be considered as function formula performing certain business process. Basically, SOA is a group of services connected "flexibly" with one another (i.e one application can "talk" to another application without knowing technical details inside), there is communication defined clearly and independently of system background, and can be reused. SOA focuses on business process and uses communication standard to hide technical sophistication below. Service orient architecture (SOA) offers methods and rules to design software as the direction of interaction with service. Service is both a basic definition and the most important part of SOA. In the model of SOA, service is defined simply as a software module or a complete program structured to connect to one another through the way of exchanging messages. Each service corresponds with one business function.

In the software system, service orient architecture is a trendy design. Service is a module of software, performing a certain business function. A service orient interaction always includes a pair of partners: Server and Client. Communicating service through the pair of request - respond. Model of SOA describes service orient communication. Broker plays a part of mediating, keeping the information of server and information of services from that server. The information is registered by the server. Users request a service; they search for information from the broker. With the information obtained, they call connection to server. When connecting successfully, they can use available services. The advantages of service orient architecture are flexibility and reusability as SOA includes a group of services with high independence.

1.2 OPC UA

OPC UA developed based on service orient architecture (SOA). OPC UA Servers describe all their functions as a group of services that Client uses. OPC UA shows what these services do and how to use them. In the meanwhile, Server side provides services and Client is the side of using services. Services determine data telecommunication at level of application. Services are the ways Client uses to access to data on information model of Server. Traditional OPC standard only defines API function, but UA defines services to determine communicative interface between UA applications. Services are independent of transporting protocol and programming environment, which is basically different from traditional OP and from API defined based on certain devices.

OPC UA service is used to exchange large sized data between progresses or between internet nodes in order to reduce transmitting among applications. Service uses the form of request – respond. To call a service in Server, Client sends a request message to Server. After having processed, Server sends respond back to Client. As this message exchanging does not happen at the same time, calling service is not at the same time, either. After sending request message, Client application can handle other functions until the responding message is delivered.

OPC is the organization offering standards based on the area of industry. OPC UA is the latest generation of OPC; the first version came into life in 2006. It does not remove the former standards but inherits all of the functions that traditional OPC standards have. Moreover, OPC UA overcomes the disadvantage of depending on COM/DCOM technology of Microsoft. It can run on .NET, Linux or Embedded device [9, 10]. OPC UA is designed based on service orient architecture, after which Servers describe their function as groups of services. Client and Server exchange through the pair: request - respond.

UA Server registers to Discovery Server its information and services it provides. Discovery Server is also an OPC UA Server. Thus, not all OPC UA provide all services. Discovery Server only provides the service which saves registration and stores information of other UA Server. Client searches for information on Discovery Server. When getting the information, Client sends request to Server. Server responds to Client. Then Client can use services that Server provides [11].

Message transmitted between Client and Server will have the format of UA Binary or XML. UA Binary encodes data in turn into a plate of byte. The advantages are reducing the cost of encoding and decoding but only OPC UA Client can translate the data in this format. Therefore, people often use UA Binary to exchange data on the equipment floor due to requirement of high productivity and limitation of handling capacity. XML is a popular method to exchange data at high level. Client uses the format of XML and OPC UA Client can both read this type of data. Data in the format of XML calculate more costly than UA Binary.

OPC UA uses protocol of OPC.TCP or SOAP/HTTP(S) to transmit. OPC.TCP is a protocol based on TCP (sockets). It defines a double channel between OPC UA Server and Client. Messages are packed into a structure as the rule of binary protocol OPC TCP. Only OPC UA Client has ability of receiving data through this protocol. SOAP/HTTP (S) packs messages into SOAP and transmits through HTTP(S).

Message SOAP is a document of XML. All the messages are transmitted through HTTP or HTTPS depending on the end point and requiring security. SOAP/HTTP(S) is an industrial standard used to exchange information on the application floor. Client Web service in general can receive SOAP message through protocol of HTTP(S).

UA Binary + OPC TCP: is the most optimal method to format and transmit the data. Consequently, this is a combination with highest possibility to be used on the floor of equipment. Only OPC UA Server and OPC UA Client can exchange information through this method.

XML + SOAP/HTTP(S): this is a friendly combination and easily overcomes firewall. This method often gives priority to exchange information on the floor of application.

2 Proposed Framework Architecture for Monitoring and Controlling System

Framework for monitoring and controlling system describes all components of the system and how to communicate between the components. Apart from meeting the demand of having a joint framework designed for a monitoring and controlling system, it must follow all standards in industry. Criteria of designing framework are suggested:

- Generality: ensure spreading criterion and be a basis to design a monitoring and controlling system.
- Flexibility: ensure the flexibility in designing, operating system (system can be operated on multi-basis).
- Reusability: ensure all components be reused for other systems.
- Spread ability: inherit and develop open feature of OPC UA standard to ensure open possibility to designers and system developers.
- Advance criterion: ensure Framework be built based on advanced architecture of SOA and new industrial standard of OPC UA.
- Simplicity: the model proposed must not be too complicated, need to be easy and convenient to implement, build and design software systems.

In the architecture of Framework, Server provides services and Client uses services (Fig. 1).

Server describes all of its functions as a group of services provided for Client. Server and Client are independent on background and programming language. Interaction between them is service oriented interaction, as the pair of request – respond. Client sends request using service to Server, Server will send back the respond to Client. They do not care about which background the other side is running on, how its inside structure is, they only care about the interaction result, service. Communication between Client and Server is through protocol of SOAP/HTTP(S) or OPC.TCP. Applications of Client are various: mobile application, enterprise application, website application…

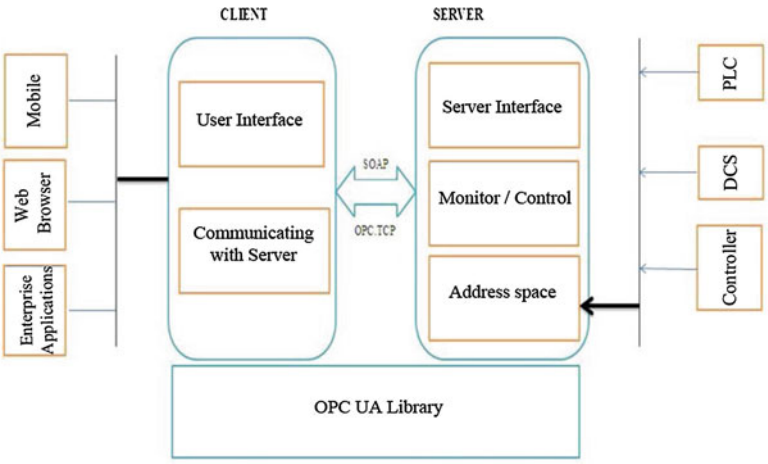


Fig. 1. Communication between Server-Client

Devices are integrated into address space of Server. In address space each device is an objective with properties and methods. Properties and methods are different from different objectives.

Tasks of the system are monitoring and controlling objectives (devices). Server provides services of monitoring and controlling them. Client searches for Server on Discovery Server, then setting connection. Communication with Server from Client allows it to use services Server provides. Users through interface of Client affect Server or devices. Client and Server programs are built based on OPC UA. It provides groups of objectives, data types, patterns of relation between nodes… as background for Server and Client. Server and Client are divided into separate components and loosely interconnect. This feature improves independence and ability of reusing components. Thus, when a certain component is changed, there will be no great influence on other components.

3 Overall Security for OPC UA

OPC UA applications will run in various environments with different security requirements, threats, and security policies. In principle, an OPC UA based framework for developing monitoring and controlling system applied for using Internet environments is base of communication complying with XML, web services, and SOA [1]. The XML signature is a system to encode digital signatures in an XML document. It uses the standard and technology encoding as other signature standard. The basic of digital signature is symmetric encryption or asymmetric encryption. However, there is important problem: How can be a secret key provided to all sides safely. There are two methods which can be used: public key and secret key (Fig. 2).

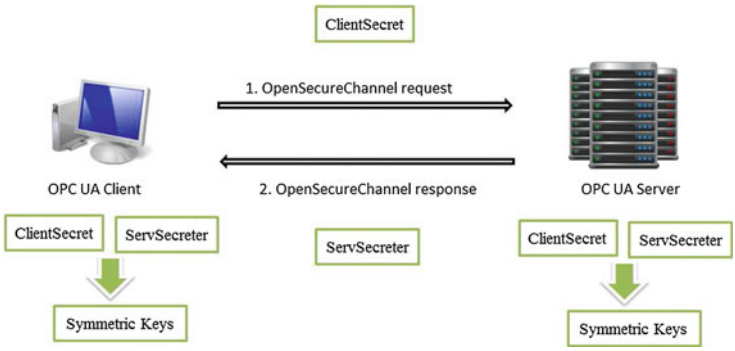


Fig. 2. Creating symmetric keys

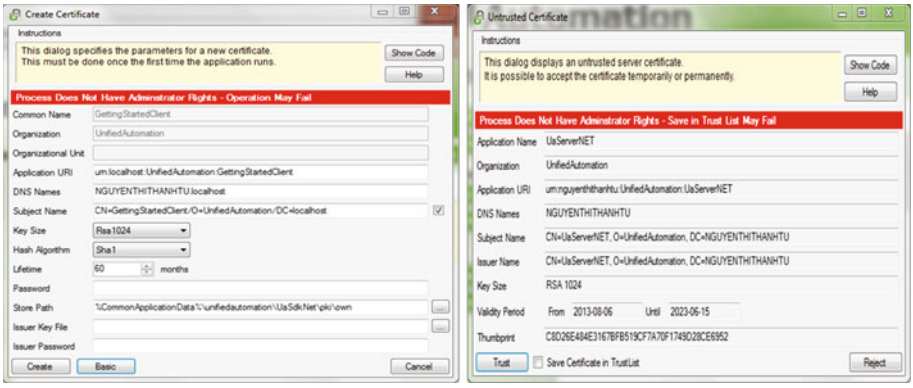
However, there is a fundamental key problem: How a secret key can be provided to the communication partner in a secure way. In contrast to symmetric cryptography, an entity in asymmetric cryptography creates a key pair in which one of them is the public key that can be safely published. The public key can be used for encrypting data and can therefore be provided to any party intending to exchange secret data. Data can be encrypted for only the private key to decipher. The private key can be also used to generate digital signatures that are used to verify the public key. The security modes in the proposed framework are "None", "Sign", and "SignAndEcrypt" [12]. For example, in the case of Secure Channel request, if security mode Sign is used, the message is signed with the private key of the client. Signing messages allows detecting a received message that has been manipulated by an untrusted third party. If security mode SignAndEncrypt is used, then the message is additionally encrypted with the public key of the server. For example, once the secured message is received by the OPC UA server, it first validates the OPC UA client's Certificate by requesting its Validation Authority. This certificate is provided in an unencrypted part of the message and therefore can be read by the server. The message is decrypted with the associated private key of the OPC UA server and the signature is verified with the public key of the OPC UA client if the certificate is trustworthy by the server. The OPC UA server sends back the response to this request, which is similarly secured. Therefore, the same checks on the message and the server certificate are performed onthe OPC UA client side.

The connection establishment between an OPC UA client and an OPC UA server includes four steps that are: First step, an OPC UA client informs itsefl about the different configuration options of how a connection to the server can be established. The second step an OpenSecureChannel request secured in accordance to the Security Policy and the Security Mode is sent to the selected Session Endpoint of the server. The third step is to create a Session on top of the previously established Secure-Channel. If the certificates are trusted by the client, the server provides the needed capabilities and proved that it possesses the correct certificate then it proceeds to the fourth and last step [12].

In this research, when OPC UA client connect to server, server will send confirm message client, after that client create a confirmation certificate and encrypt by using public key of server and send it to server, Server will confirm OPC UA client. This message is decoded by OPC UA's secret key and the digital signature will be authenticated by public key of OPC UA client. If this message is reliable, OPC UA confirms a connection by sending other message. In the next step, client save that certificate of confirmation and it does not need to create again. The result of research from apply security mechanism namely Certificate Management for proposed architecture.

Besides, RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. In this research, security solution applied RSA authorihm, there are 2 kinds: RSA 1024 and RSA 2048 - the length of KEY. Depending on the length of KEY which is short or long, if longer, the security level will be higher (see Fig. 3). Figure 3(a): Creating Certificate of confirmation (including application name, the encryption algorithm, validity period of confirmative certificate) Fig. 3(b): Certificate of confirmation (after server accept the certificate of confirmation from client. Client will save it for the next connections):

OPC Security will define access method from client to server following a specify way to protect those data and avoid every unauthorized actions. Application OPC Security specification – Certificate Management security mechanism proposed in the framework, the author developed the authentication servers and clients through using the certificate of confirmation of clients. When this certificate is authenticated, Client got a permission to connect to server. In the next connections, client using created certificate of confirmation and does not need to create it again.



(a) **(b)**

Fig. 3. (a) Create certificate (b) Untrusted certificate

4 Conclusions and Future Work

Through this research, we proposed a direction to do research, develop framework applied generally for system of monitoring and controlling automatically in industrial manufacture. We have introduced the overviews of security solutions are widely applied in automation and monitoring systems. Framework based on SOA follows the industrial standards of OPC UA to monitor, control various and complicated industrial systems bringing about flexibility in operating system, high effectiveness in management. This is a new research based on available information infrastructure of Vietnam in order to implement services of monitoring, controlling and managing manufacturing units automatically following advanced standards provided by OPC UA. Orient towards applying information technology and high technique into industrial area, which is a key area in the career of modernizing our country. Over the results of doing research and experiment, it proves that our research direction of developing framework is of highly possible implementation and brings about many practical benefits when applying in real manufacture. Orientation of future development: continue to do research and master new trends of industrial standards so as to widen and complete the model of framework much more. Coordinate with units of manufacturing automatically to implement the application of framework with a view to improving flexibility in manufacture and modernizing management, reducing cost of labor to manage and operate the system.

References

1. Damm, M., Mahnke, W., Leitner, S.-H.: OPC Unified Architecture. Springer, Berlin, 339 p. (2009)
2. Stopper, M., Katalinic, B.: Service-oriented architecture design aspects of OPC UA for industrial applications. In: Proceedings of the International Multi-Conference of Engineers and Computer Scientists, vol. II, IMECS 2009, Hong Kong (2009)
3. Leitner, S.-H., Mahnke, W.: OPC UA – Service-oriented architecture for industrial applications. http://pi.informatik.uni-siegen.de/stt/26_4/01_Fachgruppenberichte/ORA2006/07_leitner-final.pdf
4. Van Tan, V., Yoo, D.-S., Yi, M.-J.: A SOA-based framework for building monitoring and control software systems. In: Huang, D.-S., Jo, Kang-Hyun, Lee, H.-H., Kang, H.-J., Bevilacqua, V. (eds.) ICIC 2009. LNCS, vol. 5755, pp. 1013–1027. Springer, Heidelberg (2009)
5. http://www.unified-automation.com/
6. http://www.opcfoundation.org/
7. http://www.advosol.us/
8. Singh, M.P., Huhns, M.N.: Service Oriented Computing: Semantics, Processes, and Agents. Wiley, Chichester (2005)
9. Zeeb, E., Bobek, A., Bohn, H., Golatowski, F.: Service oriented architectures for embedded systems using devices profile for web services. In: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 956–963. IEEE Press, Los Alamitos (2007)

10. Jammes, F., Smit, H.: Service oriented architectures for devices the SIRENA view. In: Proceedings of the 3rd IEEE International Conference on Industrial Informatics, pp. 140–147 (2005)
11. Van Tan, V.: A SOA based framework for building monitoring and control software systems, doctoral dissertation. University of Ulsan, Korea (2010)
12. Lange, J., Iwanitz, F., Burke, T. J.: OPC - From data access to unified architecture. Vde Verlag GmbH; 4. Auflage edn (July 1 2010)
13. Tu, N.T.T., Cuong, N.D., Van Tan, V., Thang, H.Q.:Research and development of OPC client – server architectures for manufacturing and process automation. In: Proceedings of SoICT, Vietnam, 27–28 August 2010, ISBN: 978-1-4503-0105-3, pp 163–170
14. Tu, N.T.T., Thang, H.Q.: Development of an OPC UA SDK based WCF-technology and Its deployment for environmental monitoring applications. First International Conference, ICCASA 2012, Ho Chi Minh City, Vietnam, 26–27 November, 2012, Revised Selected Papers. Series: Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, vol. 109, pp. 347–356. ISBN 978-3-642-36642-0
15. XML Encryption Syntax and Processing: W3C Recommendation. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/. Accessed 10 Oct 2002
16. XML-Signature XPath Filter 2.0:W3C Recommendation. http://www.w3.org/TR/xmlenc-core. Accessed 8 Nov 2002
17. XML Signature and Processing: Recommendation. http://www.w3.org/TR/-2002/REC-xmlenc-core-20021210/. Accessed 12 Feb 2002