Secure Communication in Industrial Automation by Applying OPC UA

Stefan-Helmut Leitner, Wolfgang Mahnke, Ragnar Schierholz

ABB Corporate Research Center
stefan.leitner@de.abb.com
wolfgang.mahnke@de.abb.com
ragnar.schierholz@ch.abb.com

1. Security in Industrial Automation

Cyber security for Industrial Control Systems (ICS) has become a much discussed topic in the recent past. Despite the lack of solid data on incidents and attacks available for research there is common agreement among the experts that ICS need to better address cyber security [DNV05][BH03][NAE04][BCE02]. Regulations such as NERC CIP reflect this need and standards such as ISA 99/IEC 62443 or IEC 62351 are trying to help the industry to achieve better security levels [NAE05]. Very recently, the number of presentations on hacking ICS at the well-established hacking conferences has increased and general security researchers are more and more identifying ICS software products as a promising target for their analysis and in consequence the number of disclosed vulnerabilities in ICS products has increased significantly as well – increasing pressure on the industry even more.

Two related trends increased the security risk in ICS. ICS use more and more commercial off-the shelf (COTS) technology (usually enterprise or Internet computing) and are increasingly interconnected with other ICS and non-ICS systems. Organizations which use ICS are usually primarily concerned about their physical process (e.g. a manufacturing plant), the data and communication are merely a means to keep that process running safely and reliably. Thus, often security controls typically used in enterprise systems don't work well in ICS contexts. Conflicting interests can be observed, e.g. generally an enterprise security systems is designed to fail closed in order to protect security even when the designed control fails. However, this may lead to unsafe failure in ICS contexts when the safety systems relies on a component but a fail-closed security system blocks its availability. Given the significant advantages achieved by using COTS (cost savings, flexibility in integration), the security risks have been (more or less consciously) accepted by ICS vendors and ICS users. Only in the past years, the ICS community has started to discuss and address ICS security.

One example of the introduction of COTS into the ICS domain is OPC. OPC is based on Microsoft Windows ™ technology such as DCOM and is often used in ICS to interconnect different ICS components with each other or to interconnect an ICS with enterprise systems such as enterprise resource planning (ERP) or manufacturing execution systems (MES). However, OPC is a relatively complex set of technologies which leads to the risk of misconfiguration [BC07a]. Vulnerabilities inherent in OPC and common misconfigurations have been analyzed in [BC07b] – some of which are inherited from the COTS technology, others are inherent in the OPC design. The threats an OPC system is exposed to due to these shortcomings can range from accidental damage done by general, untargeted malware to very targeted, focused disruption of the controlled process – including consequences such as safety incidents or significant damage to equipment and the environment. While there are guidelines and recommendations for secure OPC deployment [BC07c] these are often not followed in practice (partially because they require significant effort to deploy and maintain) and they can only mitigate some of the risk.

2. OPC Unified Architecture

OPC UA [MDL09] is developed by the OPC Foundation and standardized by the IEC 62541. The predecessor of OPC UA – called classic OPC, is well accepted and implemented in almost every system targeting industrial automation. OPC UA unifies the functionality of the classic OPC specifications and brings them to state-of-the-art technology using service-oriented architecture.

Defined by OPC UA is the transport protocol as well as information modeling capabilities. The information modeling capabilities provides object-oriented features like types, inheritance, methods, etc. and can be used to define simple or complex information models. By using the information modeling capabilities of OCP UA semantic can be put into the data exchange by providing meta data like information of the device delivering the measured values, etc. There are already several standardized information models based on OPC UA for example for analyzer devices or IEC 61131-3 programming languages.

The transport protocol of OPC UA provides a robust and reliable communication infrastructure having mechanisms for handling lost messages, heartbeat, failover, etc. Using binary-encoded data, OPC UA offers a high-performing data exchange solution. Security is built into OPC UA and has been a design goal from the beginning of the development. OPC UA offers different technology mappings basing either on TCP / IP or on SOAP based web services.

Security is built into OPC UA and has been a design goal from the beginning of the development. Based on an extensive security assessment the OPC UA standard defines a consistent security model (see Figure 1) addressing security goals at different layers of the protocol stack.

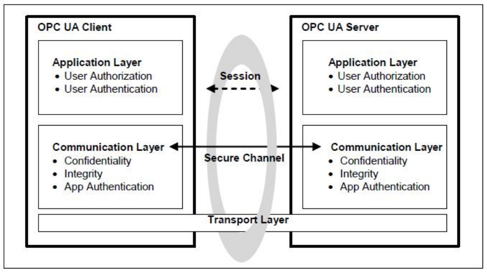

Figure 1: OPC UA Security Model [UAPart2]

At transport layer the OPC UA protocol allows recovering from broken connections while keeping the state on both client and server side. On top of the transport layer a secure channel is used to protect messages from unauthorized changes and eavesdropping by applying encryption and digital signatures. Furthermore this layer also uses authentication mechanisms based on digital certificates to authenticate and authorize individual instances of OPC UA applications. This allows administrators to establish a fine-grained access control in critical infrastructures such as production facilities and power plants. A session used for exchanging payload representing plant information (e.g., valve status, temperature, status of level indicators), settings, and commands. Session messages are therefore secured by the secure channel mentioned above. Users intending to establish sessions on the client side need to be authenticated and authorized by OPC UA servers. The specification allows three different mechanisms: Username/password combinations, digital certificates, and WS* compliant user tokens.

The OPC UA protocol is defined in an abstract manner and needs to be mapped to concrete technologies. Beside technology mappings for the transport layer as described above [UAPart6] specifies also mappings for the secure channel. For this purpose OPC UA relies on existing approved technologies like WS-Secure Conversation [WSSC] and UA Secure Conversation (which is a TLS/SSL protocol with minor adaptations).

3. Conclusion

OPC UA tries to address increasing concerns of ICS security issues and overcomes the deficiencies of “classic” OPC. Since security as an important design goal and therefore an inherent part of the OPC UA protocol. In contrast to “classic” OPC it applies strong mechanisms for authentication, data encryption and integrity. Furthermore, OPC UA does not rely on a single technology anymore. The idea of defining abstract services and technology mappings allows being flexible in future. New technology mappings can be defined for emerging and more secure technologies.

Although a lot of security-related issues are addressed by OPC UA there are still some relevant topics that are intentionally left out of the specification. One example is the lifecycle management of digital certificates. However, this topic seems to be a real challenge for the industrial automation community since it is new to this domain and not so easy to apply for automation systems.

4. Literature

[MLD09] Mahnke, W., Leitner, S.-H., Damm, M.: OPC Unified Architecture. Springer-Verlag, Berlin, 2009.

[ML09] Mahnke, W, Leitner, S.-H.: OPC Unified Architecture – The future standard for communication and information modeling in automation. ABB Review 03/2009, 2009; p. 56-61.

[DNV05] D. Dzung, M. Naedele, T.P. Von Hoff, and M. Crevatin, “Security for industrial communication systems,” Proceedings of the IEEE, vol. 93, 2005, p. 1152–1177.

[BH03] E. Byres and D. Hoffman, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, 2003.

[NAE04] M. Naedele, “IT Security for Automation Systems,” Industrial Information Technology Handbook, R. Zurawski, ed., CRC Press, 2004.

[BCE02] E. Byres, J. Carter, A. Elramly, and D. Hoffman, “Worlds in collision: Ethernet on the plant floor,” ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society, 2002.

[NAE05] M. Naedele, “Standardizing Industrial IT Security A First Look at the IEC approach,” Proc. 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 05), IEEE Computer Society, 2005.

[BC07a] E. Byres, J. Carter, M. Franz, W. Henning, J. Karsch, and P. Pedersen, OPC Security White Paper #1 - Understanding OPC and How it is Deployed, 2007.

[BC07b] E. Byres, J. Carter, M. Franz, and P. Pedersen, OPC Security White Paper #2 - OPC Exposed, 2007.

[BC07c] E. Byres, J. Carter, M. Franz, and P. Pedersen, OPC Security Whitepaper #3 - Hardening Guidelines for OPC Hosts, 2007.

[WSSC] OASIS, WS Secure Conversation 1.3, 2007, http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html