Cybersecurity of OPC ua based cyber-physical systems

Tsvetelina Ivanova, Yordan Belev, Idilia Batchkova
Dept. of Industrial Automation, University of Chemical Technology and Metallurgy
Bul. Kl. Ohridski 8, Sofia, Bulgaria

t.ivanova@uctm.edu, idilia@uctm.edu

***Abstract**: The IEC-62541 (OPC UA) standard is an important part of the Industry 4.0 reference architecture and is recommended as the only possible communication standard. A particularly important issue that is being addressed is the issue of security. Cyber security is one of the most important challenges for achieving the objectives of the Industry 4.0 initiative and of the associated cyber-physical systems (CPS). The paper analyzes the vulnerability of cyber-attacks and the main threats that threaten the security of OPC UA-based CPS and defines proven and sustainable recommendations for increasing the security of these applications.*

***Keywords**:* CYBER SECURITY, CYBER-PHYSICAL SYSTEMS, OPC UA, IEC 62541, INDUSTRY-4.0

1. Introduction

The rapid development and widespread penetration of information and communication technologies in the industry has led to the emergence of new strategies for the development of the industry in order to increase its competitiveness, such as the German initiative "Industrie 4.0" [1]. Standardization plays a central role in successfully tackling new challenges. The development and adoption of standards reduces the risk for enterprises and encourages the adoption of new technologies, products and production methods. The Industry Perspectives 4.0 study [2] confirms that the first major challenge related to the implementation of the vision is standardization. The main advantage of using standards is that they reflect the state of science and the development of technology and promote mutual understanding and consensus between partners.

Cyber-Physical Systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core [3]. Their components can be distributed both spatially and temporally, and include complex networks of feedback controllers and real time communication. These characteristics of CPS significantly complicate the cyber security of these systems and require the solution of a series of complex tasks with the application of a combination of various methods and techniques. Cyber security professionals are facing increasing challenges, both in terms of the frequency with which cyber threats occur and in terms of increasing their risk. The impact of malware and cyber-attacks can not only lead to denial of service or theft and diversion of information, but also affect the behavior of the object under control by causing it to behave in a dangerous manner, which can cause accidents and dangerous consequences. With the increasing complexity of cyber-physical systems and system of system, the issues of ensuring the security and safety of these systems are of global importance. There are three main approaches in achieving cyber security: (i) building and using reference architecture, (ii) developing cyber security standards and (iii) applying methods and tools in the field of automation in cyber security systems.

The basic requirement to the CPS for building fast, platform-independent, scalable and secure communications, which can be integrated horizontally and vertically, is fully met by the IEC-62541 standard (OPC UA) [4]. This standard defines a common infrastructure model for information exchange between components (sensors, mechanisms, control systems) and systems (MES, ERP) in the industry. OPC UA supports the following specifications: (i) information model for presenting structure, behavior and semantics; (ii) modeling of messages for interactions between applications and (iii) communication model for data transfer between endpoints. The IEC-62541 standard (OPC UA) is present in the reference architecture for Industry 4.0 - RAMI [5] and is listed as the only recommended communication standard for implementation. Two aspects are the focus of attention in this standard: the use of information modeling tools and the security issues that are covered in the standard. The paper focuses on Part 2 of IEC-62541 (OPC UA) standard [6], which addresses the security issues of OPC UA applications.

The main purpose of the paper is to analyze the vulnerability of cyber-attacks and the main threats that threaten the security of OPC UA based cyber-physical systems and to define proven and sustainable recommendations for increasing the security of these applications. These recommendations are essential for defining and using effective scenarios to increase the security of these applications and create a successful lifecycle model for the development of OPC UA based cyber-physical systems.

The paper is structured in 4 parts. Following the introduction, in part two, the IEC-62541 (OPC-UA) standard, the term security and the security model are briefly presented. Part 3 provides a brief analysis of cyber-attack threats that threaten the security of OPC UA applications. Part 4 systematizes the main recommendations for building secure OPC UA based cyber-physical systems, which can be used to improve their development lifecycle model.

2. OPC-UA and the security model

2.1. Summary of IEC-62541 standard (OPC-UA)

The IEC-62541 standard or also known as OPC-UA (Open Platform Communication - Unified Architecture) [4], which includes 14 parts, presents a new generation of OPC, which replaces TCP/IP communication protocols specific to DCOM, allowing: (1) the use of OPC applications on any operating system; (2) the implementation in all languages; (3) the use of OPC in devices (firmware); (4) to activate WAN (secure Internet/Intranet/Extranet) and (5) to improve the security management. OPC UA combines all previous protocols into a common, unified data model. It offers a complete networked, object-oriented concept for the namespace, including metadata for defining objects. The OPC UA specification defines a service-oriented architecture (SOA) with a set of services described in Part 4 of the standard [7]. The information models in OPC UA form a layered structure, shown in Fig. 1, where the basic information model is at the lowest level. Above the base model are service-specific extensions to the information model for data access, alarms and conditions, programs, historical access, and aggregates. The accompanying specifications are defined above the composition of the general information models. The next layer contains the accompanying specifications, which are domain-specific information models. At the top level of the OPC UA structure, highly refined information models from different companies or suppliers for use in their specific products are defined. The composition of information models can be extended. The information models are defined and explained in Part 5 of the standard [8].

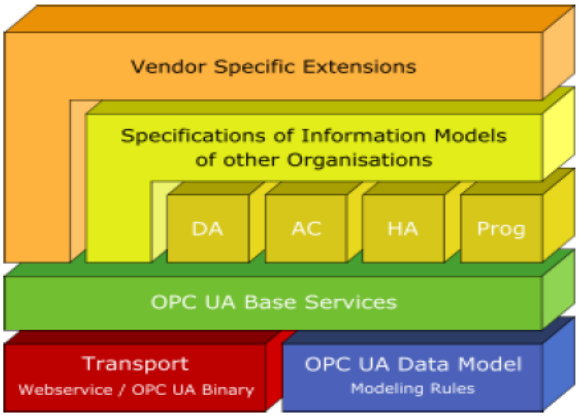

Fig.1: *Multilayer structure of models in OPC UA [8]*

With OPC UA, OPC Foundation makes the transition from object-oriented COM/DCOM technology to service-oriented architecture by integrating previous specifications into a single address space represented by a model for defining complex information in the form of objects consisting of nodes, connected with references. Different classes of nodes convey different semantics. For example, a variable node is a readable or writable value, which has an associated data type that can define the current value. The method node is a function that can be called to be executed. Each node is characterized by attributes, including a unique identifier.

2.2. On the definition of security

In the English technical literature, there are two terms for software security - "assurance" and "security". The term "assurance" looks at security in a broader sense, including its reliability, also known as software resilience, software safety, and its security as "Security", which is the ability of software to resist, tolerate and recovers from events that intentionally compromise its reliability. According to the US National Security Systems Committee's (CNSS) National Information Security Dictionary [9], software security is: "the degree of assurance that software is free of vulnerabilities, either intentionally designed in the software, or accidentally included in any time throughout its life cycle, and that the software functions as intended". Achieving software security affects all phases of the software development life cycle, and the goal of all integrated activities in this direction is to achieve software that shows:

- Trustworthiness - mainly related to the absence of malicious and/or unintentional operational vulnerabilities or weaknesses;
- Predictable execution - there is reasonable assurance that the software, when executed, functions only as intended;
- Conformance - where a planned and systematic set of multidisciplinary activities ensures that software processes and products meet the relevant requirements, standards and procedures.

2.3. Security objectives in OPC-UA

The security model is presented in Part 2 of IEC-62541 [6]. The security of industrial systems is achieved by achieving a set of objectives that are defined on the basis of many years of experience and remain unchanged over the years, despite the ever-changing set of threats to the systems. The main objectives of security are summarized as follows:

- Authentication (A1): Entities such as clients, servers and users must prove their identity. Authentication can be based on something that the entity is, possesses or knows;
- Authorization (A2): Access to read, write or execute resources should be allowed only for those objects that need this access within the system requirements;
- Confidentiality (A3): ensures that users without access rights do not have access to the information, i.e. the data is protected from passive attacks such as eavesdropping, whether the data is transmitted to be stored in memory or stored. To ensure confidentiality, data encryption algorithms using special data protection secrets are used, along with authentication and authorization mechanisms to access this secret;
- Integrity (A4): refers to maintaining the accuracy and integrity of the information, i.e. the recipients receive the same information as the original sender, without the data changing during transmission. Unauthorized changes by authorized organizations or any modifications by unauthorized entities, such as: overwriting, falsification, destruction, involuntary or malicious insertion of logic, deletion, etc. should not be allowed;
- Auditability (A5): actions taken by the system should be recorded to provide evidence to stakeholders that the system is working as intended (successful actions are tracked), to identify the initiator of certain actions (the activity of the user is tracked), to find that attempts to compromise the system have been denied (unsuccessful actions are tracked);
- Availability (A6): refers to the ability of authorized persons to have access to information and timely maintenance of information resources in a state in which they can be used without problems.
- Non-Repudiation (A7): non-repudiation ensures that something that actually happened cannot be said not to have happened. The security service that provides this protection can be one of two types: (1) the recipient of the data receives and stores information proving that the data came from the creator. This blocks the author from claiming that he never sent the data. (2) one in which the sender of the data receives confirmation that the data have been received by the recipient as intended.

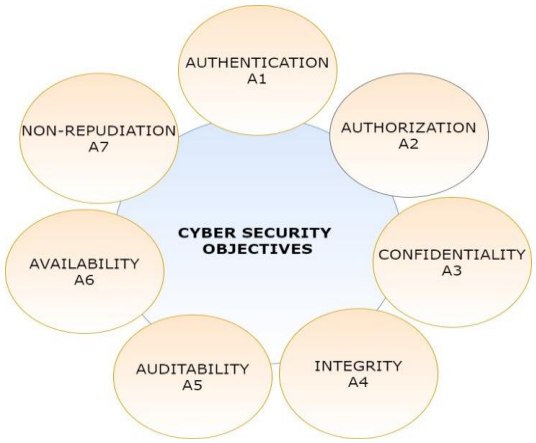

Fig.2: *Cyber security objectives*

Based on the requirements for confidentiality, integrity and availability, a classification of systems and data has been developed, and classes have been defined in accordance with the quality aspects of these requirements. Each class meets a minimum set of security requirements to be met and security measures to be taken. At the heart of this classification are the ISO27001 and ISO27002 standards. The ISO27001 standard refers to the requirements for information security management systems, preparation or selection of lists of known risks, based on various sources of good practice, such as CAPEC (contains a list of 1000 possible attacks), Microsoft's STRIDE, OWASP "Top 10" and many others.

Security is achieved through preventive methods used to protect information from theft, compromise or attack. This requires understanding potential information threats such as viruses and other malicious code. Security risk is a product of three elements: threat, vulnerability and impact. Risk refers to the possibility of loss or damage when a specific threat exploits a captured vulnerability. Risk can include financial losses as a result of business interruptions, damage to reputation, legal

consequences and even loss of life. Vulnerability refers to a specific weakness in assets (resources) that allows a particular attack to be successful.

2.4. OPC-UA security architecture

The standard provides a flexible set of security mechanisms. Client-server communication can be realized in two ways - through and without a session, as shown in Fig. 3. The session is organized in the application layer and in addition to the routine work of client and server applications. It has the task of managing the security, authentication and authorization objectives of the user. The session communicates through a security channel in the communication layer, which is organized in a very flexible way and must be activated. The communication layer provides security mechanisms to achieve confidentiality, integrity, and authentication of the application, using a secure channel that provides encryption to maintain confidentiality, signing messages to maintain integrity, and application authentication certificates. The security mechanisms provided by the Secure Channel services are implemented by a stack protocol that is selected for execution. When OPC UA (UACP) protocols are used, then the security functions are specified in the SSL/TLS mode.

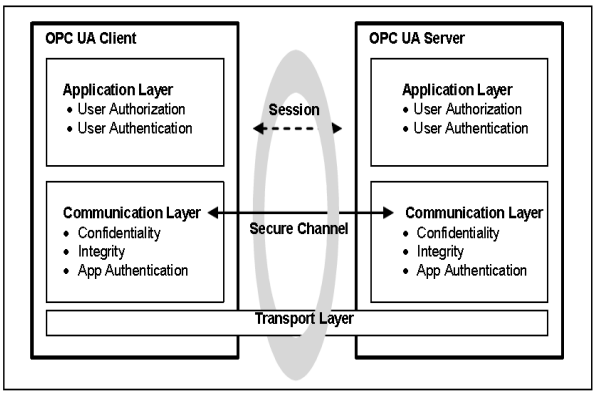

Fig.3: *OPC-UA security architecture for client-server applications [6]*

Communication between applications is based on messages, the parameters of which are defined in Part 4 of the standard and their format defined by *Data Encoding* and *Transport Protocol* (Fig. 4). A stack is a collection of software libraries that implement one or more *Stack Profiles*. The interface between the application and the stack hides the details of stack execution, depending entirely on the development platform used. Each OPC UA *Stack Profile* is a separate application protocol. Even when *Security Mode = None* is selected, i.e. security is not supported, the *Secure Channel* layer is present, supporting a logical channel with a unique identifier.

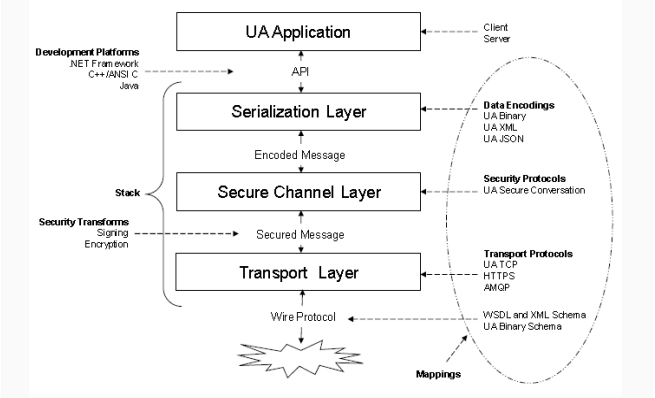

Fig.4: *OPC-UA security architecture for client – server applications*

3. Analysis of threats to OPC UA based CPS

3.1. Defining the main threats

The security of cyber-physical systems reduces the risk of damage caused by attacks. This includes: (1) identifying system threats, (2) identifying system vulnerabilities to those threats, and (3) providing countermeasures that directly reduce vulnerabilities, counter threats, or recover from successful attacks.

OPC UA applications can be used in a variety of operating environments. In some cases, they can be an attractive target for industrial espionage or sabotage, and they can also be exposed to threats through unobtrusive malware, such as worms circulating in public networks with different assumptions about threats and accessibility, as well as different policies for security and application modes. Some of the most common threats to OPC UA based CPS can be summarized as follows:

- Message Flooding: The attacker sends a sequence of requests to the system in an attempt to consume enough server resources to make the system insensitive to legitimate traffic.
- Eavesdropping: listening to other people's conversation or communication without their consent.
- Message Spoofing: A malicious party that impersonates another device or user on the network to launch attacks on network hosts, steals data, distribute malware, or bypass access controls.
- Message Alteration: during the attack, messages are intercepted in the communication environment, and certain information can be changed, or the call can be diverted, the service can be interrupted, etc.
- Message Replay: A network attack in which a valid data transmission is recorded and then played back to affect system operations.
- Malformed Messages: Also known as Protocol Fuzzing, the attack sends messages with the wrong syntax to the target server or client to interrupt the service.
- Server Profiling: Gathers information about the server or related equipment to explore what the core infrastructure is.
- Session Hijacking: When a TCP session is hijacked, the user session is attacked over a secure network. Session hijacking is also known as a "middle man attack" in which an attacker uses a computer program (sniffer) that detects and records a variety of limited information, especially secret passwords needed to access files or networks.
- Rogue Server: A rogue server is a network server that is not under the administrative control of network personnel.
- Compromised User Credentials: User credentials are available to others other than the user (without their knowledge or consent) and may be logged into the user's account.

3.2. Coordinating threats with OPC UA security mechanisms

The coherence achieved between the threats and the security mechanisms of OPC UA, presented in Table 1, links the security functions of OPC UA with specific threats. For example, the following cases are possible (1) OPC UA minimizes the loss of availability caused by flooding with messages by minimizing the processing of messages until they are authenticated, or (2) when eavesdropping occurs, OPC UA provides encryption to protect against eavesdropping, or (3) OPC UA counts threats to tamper with messages by providing the ability to sign messages, or (4) OPC UA counteracts session hijacking by setting a security context, i.e. security channel in each session, etc.

Table.1: *Consistency of threats and security functions*

Threats	A1	A2	A3	A4	A5	A6
Message Flooding						X
Eavesdropping			X			
Message Spoofing		X		X		
Message Alteration		X		X		
Message Replay		X				
Malformed Messages				X		
Server Profiling	X	X	X	X	X	X
Session Hijacking	X	X	X			
Rogue Server	X	X	X		X	X
Compromised User Credentials		X	X			

4. Safety recommendations when using OPC UA

As a result of a number of tests performed in accordance with the standard, the following recommendations have been identified and summarized with a view to the use of secure communications with the OPC UA protocol:

• Operation in "*SecurityMode*": This means that "*Sign*" or "*SignAndEncrypt*" mode must be selected. These modes ensure that, at the application level, authentication is mandatory. "*None*" security mode does not provide protection! The "*SignAndEncrypt*" security mode is used to protect the integrity of data and its confidentiality [10].

• Choice of cryptographic algorithms: "*Basic256Sha256*" must be selected as the *SecurityPolicy* [11], provided that the clients with which the server interacts support this policy. Security policies using outdated algorithms, such as "*SHA-1*", should not be used.

• User authentication: Logging in to the UA server with an "anonymous" ID should only be used when accessing non-critical resources, as in this case it is not possible to track by the server who is changing the data or configuration. Hackers can take advantage of these recommendations to use OPC UA with a Secure Way ID to read or write data in an unauthorized manner. This can happen if the restriction on the rights to work with the "anonymous" identifier is not configured adequately. [10]

• Storing certificates and private keys: The used private keys or certificate files should not be stored in an unencrypted file system. For this purpose, special certificates stores of the operating system and its capabilities for setting access rights must be used. It is recommended to use TPMs (Trusted Platform Modules) or external secure hardware, such as USB authentication tokens to store certificates and/or private keys.

• Use certificates: Connections that do not provide trusted certificates are not allowed. Self-signed certificates require additional verification. If the certificates are not self-signed, the establishment of a certification body is required, and the certificates of the certification body are signed independently or by another certification body. Certification bodies can be multi-layered [5].

• Certificate management and maintenance: It is recommended to use certificate trust lists and certificate revocation lists to manage only valid certificates. These lists are created by trusted users or processes. The lists must be updated regularly.

Conclusions

Digitalization and growing network structures and applications on the one hand, and increasing hacking attacks on critical infrastructures and industrial applications on the other, are placing the issue of network and application security increasingly on the agenda. The analysis and comparison of the capabilities of OPC UA presented in the paper show the ability to successfully deal with security issues at different levels in the automation pyramid. The defined objectives, potential threats and established compliance allow, according to IEC-62541 standard (OPC UA), the development of security profiles and models for individual areas of application.

Acknowledgment: The study was conducted within the National Research Program "Information and Communication Technologies for a Digital Single Market in Science, Education and Security (ICTinSES)", funded by the Ministry of Education and Science.

References

1. Kagermann H., Wahlster W., Helbig J., Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report of the Industrie 4.0 Working Group, Akatech, April, 2013.
2. Forschungsunion, "Recommendations for implementing the strategic initiative Industry 4.0", Acatech, 2013.
3. Rajkumar, R., I. Lee, L. Sha, and J. Stankovic (2010), Cyber-physical systems: the next computing revolution, In Proceedings of the 47th Design Automation Conference, ACM, New York, 2010, pp. 731-736.
4. OPC Foundation (2017), OPC UA Specification, Part 1: Overview and Concepts, http://www.opcfoundation.org/UA/Part1/
5. DIN SPEC 91345, Reference architectural model Industry 4.0 (RAMI4.0), 2016, Berlin.
6. OPC Foundation (2018), OPC UA Specification, Part 2: Security model http://www.opcfoundation.org/UA/Part2/
7. OPC Foundation (2017), OPC UA Specification, Part 4: Services http://www.opcfoundation.org/UA/Part4/
8. OPC Foundation (2017), OPC UA Specification, Part 5: Information Model, http://www.opcfoundation.org/UA/Part5/
9. Committee on National Security Systems, National Information Assurance (IA) Glossary, CNSS instruction No. 4009 (revised June 2006). Available from: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
10. Fiat, Störtkuhl, Plöb, Zugfil, Gappmeier and Damm, "OPC UA Security Analysis," Federal Office for Information Security, Bonn, Germany, 2017.
11. OPC Foundation (2017), OPC UA Specification, Part 7: Profiles, http://www.opcfoundation.org/UA/Part7/