Analysis of Cyber Security for Industrial Control Systems

Zakarya DRIAS
Schneider Electric
Carros. France
Zakarya.drias@schneider-electric.com

Ahmed SERHROUCHNI
Telecom ParisTech
Paris. France
Ahmed.serhrouchni@telecom-paristech.fr

Olivier VOGEL
Schneider Electric
Carros. France
Olivier.vogel@schneider-electric.com

***Abstract*— Industrial control systems (ICS) are specialized information systems that differs significantly form traditional information systems used in the IT world. The main use of ICS is to manage critical infrastructures such as, Oil and Natural Gas facilities, nuclear plants, smart grids, water and waste water…etc. ICS have many unique functional characteristics, including a need for real-time response and extremely high availability, predictability, reliability, as well as distributed intelligence. Which for, many advanced computing, communication and internet technologies were integrated to the ICS to cover more costumers requirements such as mobility, data analytics, extensibility…etc The integration of these technologies makes from the ICS open systems to the external world; this openness exposes the critical infrastructures to several Cyber security critical issues. Nowadays, cyber security emerges to be one of the most critical issues because of the immediate impact and the high cost of cyber-attacks. In this paper, we present a comprehensive analysis of cyber security issues for ICS. Specifically we focus on discussing and reviewing the different types and architectures of an ICS, security requirements, different threats attacks, and existing solutions to secure Industrial control systems. By this survey, we desire to provide a clear understanding of security issues in ICS and clarify the different research issues to solve in the future.**

Keywords— *ICS, DCS, SCADA, Cyber security*

I. INTRODUCTION

Industrial control systems (ICS) is a large term used to describe several types of systems such as, DCS (Distributed Control systems), SCADA (Supervisory Control and data Acquisition), IAS (Industrial Automation system), IACS (Industrial Automation and Control Systems) or even PLC(Programmable Logic Controller). ICS are typically used in industries such Power plants, Water and waste water facilities, Oil and Gas refineries and distribution, Nuclear plants …etc. These control systems are critical to the operation of critical infrastructures that are often highly interconnected and mutually dependent systems. SCADA systems are a set of Software and hardware used generally in the control and monitoring of geographically dispersed assets and process (Ex: Gas Distribution) where the centralization of data acquisition and control are critical to System Operation. Where the DCS is generally focused on the automatic control of a process usually within a closed area (Ex: Gas Refineries), more details on SCADA systems are discussed in [2] .Unlike SCADA systems, DCS are connected directly to equipment that it controls, the main constrains in DCS operations is the system availability. From an operation point of view, the major difference between SCADA and DCS is the DCS relies on the ability to obtain immediately the current view of the system state, where the SCADA relies on the event reporting where all transitions in the system are reported, more details on DCS are found in [3].

Another main deference vector is the intelligence of the systems; the intelligence of DCS is distributed between the different controllers where the Intelligence in SCADA systems is the addition of all controllers' individual intelligences. Most of the ICS in use today were developed years ago, before that public and private networks, desktop computing, or the Internet are becoming a part of industrial operations.

These systems were designed to meet performances, availability, safety, and flexibility requirements using proprietary communication protocols. In most cases they were physically isolated from outside networks and based on proprietary hardware, software, and communication protocols that included, basic error detection and correction capabilities, without any security considerations. At that time, the security for ICS meant physically securing access to the network and consoles controlling the system. The evolution of IT systems increased the requirement of control systems interoperability, interconnectivity, openness and communication standardization; which conducted the system providers to integrate more and more internet technologies and protocols to ICS under the same system constraints discussed above to meet the openness requirements. The openness of ICS to Internet world by adopting IT technologies makes them exposed to new types of threats and increased the possibility that an ICS could be compromised with cyber-attacks, Some of these attacks include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses, and damages to a nation's economy. Since the security researches for ICS is still in its first steps. Therefore, our objective in this paper is to provide a deep overview and analysis on ICS architectures and communication protocols and what makes the ICS different than IT systems than focus on different threats and vulnerabilities, then review some of the most used security solutions to protect ICS and we summarize with research challenges in the ICS Security field.

II. OVERVIEW ON ICS

An industrial control system is a set of interconnected assets and subsystems in order to perform three main operations,

978-1-4673-7977-9/15/$31.00 ©2015 IEEE

acquisition, control and supervision. Depending on the target filed of application. Typically, ICS collects sensors measurements results and operational data from the process field, process, analyze, display them for system operators and executes control logic in local or remote control devices. Several standard architectures are defined by standardization organizations such as ISA [4], NERC [5], AGA [6]…etc., these architectures describe the different levels of the system from two points of view, Network and operations. In the following paragraph, we discuss two primary types of Control systems, DCS and SCADA. DCS (Distributed Control systems), are used in process and generation plants within a defined area where the interaction between the equipment needs a distributed control logic. SCADA systems are used for large and geographically dispersed facilities, typically for distribution. For example, a Natural GAS company may use DCS for GAS refinement to control refineries, and SCADA for GAS distribution to supervise the pipeline.

A. ICS Key components

Later on this chapter, we attend to present different ICS architectures. In this section, we discuss the key components to be used in ICS Architectures and implementations; those components can be used generally in both SCADA and DCS or specifically for DCS or SCADA.

1. *Control Components:*

Control server: the Control Server is software responsible of controllers (PLC) configuration; it hosts all the control logic applications and device network configuration. Additionally, it hosts some real time monitoring services. Control server is connected directly to control devices through a control network.

SCADA Server: Known in the academic literature as MTU (master Terminal Unit); which is the central device in SCADA architecture to host all supervision, control functions and data object model for the process assets.

Remote Terminal Unit (RTU): are field devices used usually in in telemetry implementations of SCADA systems. By telemetry we mean highly automated communication process where measurement and data acquisition is done remotely in inaccessible areas where wired connections are unavailable. RTUs are interfacing objects in industrial facilities to SCADA or DCS system by transmitting acquired telemetry Data and by executing control logic for a basic control for connected objects.

Programmable Logic Controller (PLC): NIST [1] defines a PLC as *"a small industrial computer originally used to perform the logic functions executed by electrical hardware* “, this definition corresponds to the first version of PLCs that appeared in mid-60’s. Nowadays PLCs are capable of controlling complex process in both DCS and SCADA systems. PLCs are able to solve a complex logic to control process functions and communications which is generated by the control server. In most of real implementations, PLCs are connected to lower levels devices such as sensors and actuators.

Intelligent Electronic Devices (IED): are industrial devices (sensors, actuators) with enough intelligence to acquire data and transmit them to PLCs, RTUs and monitoring services. The IEDs are interfacing with the field part of the process where analog communication capabilities are required for IEDs in both, data acquisition and local control.

Human Machine Interface (HMI): is software hosted in computers or in specific hardware used to monitor the process, modify control settings, and manually override control operations. HMIs could be clients of SCADA servers or directly connected to the control network.

Data Historian: is a centralized database connected to one or several MTUs, to collect all process logs and events. Set of information hosted by Historian are accessed by some big data services for data analysis to be communicated to enterprise level.

Input/output (I/O) Server: The IO server is a software component responsible for collecting, buffering and providing access to process information from control devices to be transmitted to Control and SCADA servers.

2. Network Components:

An ICS is hierarchized in different network layers, Enterprise Network, Control network, field network. The ICS components we listed above are interacting in those different levels to provide several functionalities that we discussed previously for both system implementations, SCADA and DCS. They are interconnected through network components depending on the context of usage and regardless of the topology. The evolution of control components to support IT based protocols conducted to the customization of IT network components to meet the ICS requirements such as availability, performance, etc. another reason behind using IT based networking technologies is to merge the Corporate networks with the control networks and allow the engineers to control and monitor the process control remotely outside the installation. The following is a list of main network components used in ICS networks for each layer.

Fieldbus Network: the fled bus network is connecting IEDs such as sensors, actuators and other filed devices to a PLC or other controllers. The use of specific network for field devices avoids the direct linking of sensors and field devices to PLCs. Several communication protocols are used to communicate between controllers and devices or between devices themselves.

Control Network: the control network is connecting the upper level (supervisory control, control server, monitoring services) to the controllers and RTUs.

Remote Access Points: RAPs are radio based communication devices used generally in Highly distributed SCADA implementations for remotely configure ,monitor and access remote devices such as RTUs and IEDs.

B. ICS Architectures:

In ICS implementations the components are interacting differently due to the functional scenario behind each implementation. This will be followed by communications protocols the widely used in the ICS.

a. DCS Architecture:

DCS is using centralized supervisory loops as an intermediate layer in a group of distributed controllers that share the logic of controlling the process [7]. The motivation behind using DCS is to modularize the process to reduce the single point of failures within the functional units. A DCS is architectures to 4 layers, Enterprise, Operation, Control and field layer [8].

In DCS architecture shown in figure 1, the control engineers connected to the control network design the control application. The DCS Server connected to both operation and control network downloads the application to the different PLCs. Once done, the controllers receive process variable values from the field devices through fieldbus network which conducts to execute the embedded control logic. In distributed control case, the controllers interact between them to perform a distributed logic execution. During the execution of control application in the controllers, the DCS server requests data from the distributed filed controllers and devices. Those data are graphically displayed to the Operators.

b. SCADA Architecture:

SCADA systems refer to geographically dispersed systems for telemetry control and data acquisition. The control room is the central point for SCADA systems, SCADA servers are connected to SCADA clients for displaying the process events from acquired data from the telemetry outstations. SCADA servers contain tags to all the devices connected to the control and acquisition network. The communication between SCADA servers and RTUs is ensured through different channels, wired connection, wireless or radio connection and satellite connections. In the remote sites, RTUs are connected to filed devices and PLCs through a LAN. SCADA server is providing the ability to SCADA client to perform control actions in case of untreated alarms. All the information gathered from the field are stored in the Data Historian for data analytics purposes. Figure 2 is showing a typical SCADA system architecture.

C. ICS Protocols:

Understanding how ICS work requires a basic understanding of the underlying communication protocols that are used, where there are used and why. In the Industrial automation and control sector, many specialized protocols are used. Those Protocols are designed to ensure efficiency, Reliability and precision real time operation. This means that any other inefficient functions are taken off the protocol.

Unfortunately, this usually includes the security functions and features such as authentication and encryption which expose the protocol users to a security threats. Another source of vulnerabilities is the convergence of the protocols to run over IP networks to meet the evolving needs of the business.

Depending on the type of system architecture and needed services, control, supervision, or both, many protocols are deployed these days; we cite Modbus, DNP3, OPCUA,...etc . In the following, we focus on the two most used protocols in the industrial control networks: Modbus and DNP3.

a. DNP3:

Distributed Network Protocol (DNP3) began as a serial protocol designed for use between master control stations and slave devices or "outstations," as well as for use between RTUs and IEDs within a control station. Like most of control system protocols, DNP3 was extended to work over IP, encapsulated in TCP or UDP packets, in order to make remote RTU communications more easily accessible over modern networks [9]. One distinction of DNP3 is that it is very reliable, while remaining efficient and well suited for real-time data transfer.

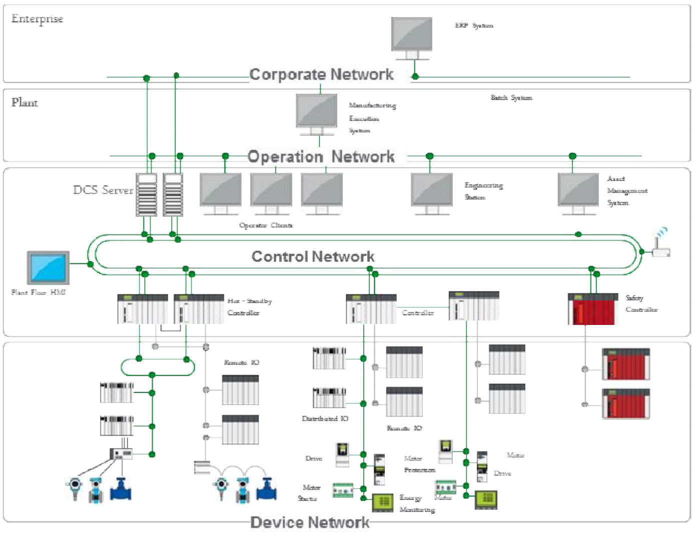

Figure 1 Typical DCS Architecture

It also utilizes several standardized data formats and supports time-stamped (and time-synchronized) data, making real-time transmissions more efficient and thus even more reliable.DNP3 is primarily used to send and receive messages between control system devices only in the case of DNP3.[10]

a. Modbus:

Modbus is the most used protocol of industrial communication protocols. It was originally designed in the mid-1970s by Modicon as a way to link intelligent devices with PLCs using a simple master/slave concept. Simple is a key descriptor for Modbus – and also its biggest strength. It is easy to implement and easy to use [10]. When it was first introduced, it was a proprietary protocol that only Modicon could use, and then it was freely published for public usage

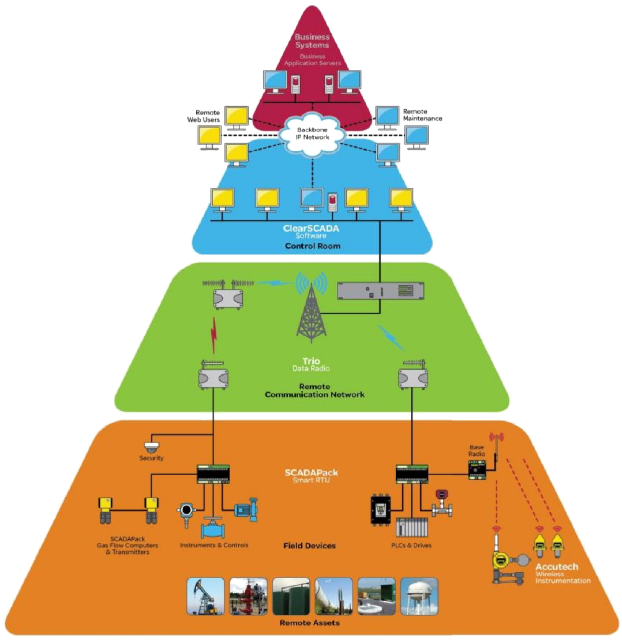

Figure 3 Typical SCADA systems Architecture

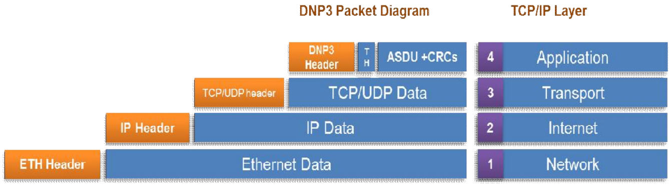

Figure 4 DNP3 Protocol Stack

Within the convergence of Control network to be IP based networks, a variation of Modbus developed over TCP application layer protocol using the port 502.As already noted, Modbus is a simple master-slave protocol. The master has full control of communication, whereas a slave will only respond when spoken to. The master will record outputs and read inputs from each of its slaves, during every cycle. The protocol is pretty basic. There is no additional requirement for the slave or master to have a watchdog timer to ensure that communications occur within a certain time. The slave devices do not “join” the network, they simply respond whenever a master talks to them. If the master never talks to them, then they are idle. There is also no requirement for diagnostics related to the slave’s health. If the master is requesting data without any sense to the slave, then the slave is sending an exception response. However, if the process variable is bad or if the device has problems functioning, there is nothing in the protocol that requires the slave to report this.

DNP3 and Modbus were designed without any security mechanism; all their messages can be intercepted and falsified or replayed, which has a very huge impact on control or supervision operations. Hence the ICS provider as well as security researchers and organizations are working together to come with secure protocols by design. Most of Security organization is coming from the Internet world with an IT oriented security knowledge. Firstly, it's very useful to make the difference between Internet and ICS and take into account that difference for an efficient security design.

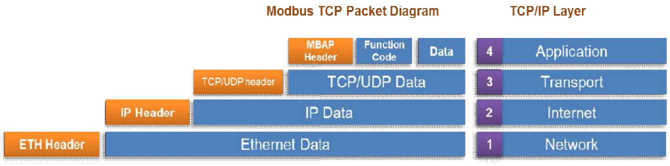

Figure 2Modbus Protocol Stack

III. SECURITY OBJECTIVES FOR ICS

Since the ICS are used to control critical infrastructures and the adoption of internet technologies by the ICS, security is becoming a real issue that ICS owner and vendors are facing to. To ensure the reliability and security of control operations, it is essential to understand the security objectives and requirements before defining any security mechanisms or countermeasures in the context of ICS. The following explains the security objective for industrial control systems.
NIST cyber security working group released a guide to secure industrial control systems, from this guide we conclude three main security objectives:

- *Availability*: Real time access to data assets is primordial to control system operations. Unavailability of system assets or interrupted control operations conducts to the loose of facility functions. In the case of critical infrastructures, it conducts to economic and human damages.
- *Integrity*: is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Integrity is a very important aspect in industrial control systems, where the any false actions due the altered data are permitted.
- *Confidentiality*: is a service used to keep the content of information from all but those authorized to have it. Confidentiality in control systems means keeping the sensitive data of the process inaccessible from unauthorized users and assets.

The most important aspect in the industrial control systems is the reliability, therefor; the availability and integrity are the most important security objectives. Confidentiality is less critical than the two other objectives. However; with the development of the ICS to be part of the global Internet of things, the ICS assets are more interacting with human user to manage their private date, in this case confidentiality becomes a critical objective.

IV. CYBER SECURITY REQUIREMENTS FOR ICS

The three discussed security objectives in the previous paragraph are high level security objectives for ICS. Several standardization and governmental organizations, such as

NERC, ISA and NIST came with a set of functional and organizational requirements to protect industrial control systems from cyber-attacks. All those requirements have a goal; the insurance of the security objectives. As we are interested by the systems security functional requirements, we summarize in the following security requirements for ICS.

- *Network Protection*:

Comparing to internet, ICS are segmented into different levels of networks in a large scale, it is almost impossible to ensure that each network node is invulnerable to cyber-attacks, avoiding attack is quite impossible. Therefore, Industrial networks should perform profiling, network traffic monitoring, and attack detections. Industrial network infrastructure must be able to ensure control operations under attacks due to the criticality of the systems that they operate.

- *Authentication and authorization*:

As discussed previously, Industrial control infrastructures may operate thousands of devices, software as well as users. Each system component must be identified and authenticated. Authentication is the key concept for identifying systems assets then, guaranteeing that they are allowed to access another resource within the system .Unlike Internet, two assets must perform mutual authentication instead of the one way authentication used in Internet world. Authorization should be integrated to industrial control systems to prevent au authorized users of services to access sensitive system resources. To have these two mechanisms within the system, cryptographic functionalities should be integrated to the system such a symmetric and asymmetric cryptography.

- *Secure communications and protocols*:

Unlike in conventional networks, exchanged messages in industrial networks require security and latency. Especially in the case of SCADA systems where the exchanges are in a large scale infrastructure geographically dispersed .Physical security of communication layers is not enough for communication security. Any miss in protocol configuration or design may conduct to the violation of security principle. Therefore, any communication between the three levels of ICS (field, plant and control room) should be secured, by adding security by design in communication protocol such as Modbus and DNP3.Note that industrial control systems are requiring much more security requirements than Internet due to the criticality of infrastructure that deploys ICS and the lake of security in initial ICS design. With the convergence of ICS to Internet of things those requirements will ease the integration of ICS to IoT architectures.

V. Security threats in Industrial control systems

It is essential to understand why cyber security is primordial for ICS. The first motivation of investigating security is the increase of attack vectors against industrial control systems, those attacks are mostly the heritage from the Internet world by the adoption of Internet technologies. In this chapter we discuss the different types of threats against ICS security; we classify them into different threat categories, then we analyze the impact of each attack on the ICS operations.

We classify attacks into three main categories: *Attacks targeting availability, attacks targeting confidentiality, attacks targeting integrity.*

- *Attacks targeting Availability*: attacks targeting availability intend to deny access to system assets as well as operations. In ICS, this refers to deny of access to all the components of a systems like the ICS assets; Operator workstations, Engineering stations, communications system as well as control devices.
- *Attacks targeting Integrity*: by illegally modifying the content of a message or the content of system assets. In ICS that becomes to modify acquired messages or control commands transiting through the three system levels as well as modifying the content of databases or control programs in PLCs or RTUs.
- *Attacks targeting Confidentiality*: their aim is to acquire unauthorized data or resources in the Industrial control network. Acquired data such as passwords, PLCs configurations may be used unintentionally to replay some ICS operations.

Those threats can exploit vulnerabilities in the design and implementation of ICS networks and communication protocols to generate several attacks already known in the IT world but with a higher impact on the process managed by the ICS. We cite in the following the most relevant attacks related to the classification above.

- *DoS*: The main goal of this attack is to decrease the availability of the system for its intended purpose.
- *Eavesdropping*: The goal of the attacker is to violate the confidentiality of the communication, e.g., by sniffing packets on the LAN or by intercepting wireless transmissions [14].
- *Man-in-the-middle*: In a man-in-the-middle attack, the attacker acts toward both end points of the communication as if the attacker was the expected, legitimate partner. In addition to confidentiality violations, this also allows modifying the exchanged messages. Via man-in-the-middle attacks, weaknesses in the implementation, or usage of certain key exchange and authentication protocols, can be exploited to gain control even over encrypted sessions [15].
- *Breaking into a system*: Through violation of the authentication and access control objectives, the attacker obtains the ability to control aspects of the behavior of the communication system and the connected plant at his will, including the ability to overcome confidentiality and integrity objectives. A break-in usually involves the consecutive penetration of multiple subsystems and the step-wise elevation of the privileges of the attacker.

Real stories-attacks have targeted the control systems of several installations such as the Iranian nuclear facility, US power utility and Saudi Aramco plants. The followings are the most sophisticated attacks identified by security researchers and experts:

a. Stuxnet

Stuxnet is a Microsoft Windows computer worm discovered in July 2010 that specifically targets industrial software and equipment of the Iranian nuclear facility [16]. The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only specific SCADA systems that are configured to control and monitor an industrial process. Stuxnet exploited several vulnerabilities in the execution environment as well as in the ICS protocol implementation [24].

b. B. Slammer Worm

The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the nuclear power plant in Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly.

c. Shamoon Malware

Is a malware attack that targeted the Saudi Aramco refineries which are the 8th largest refinery in the world. The malware targeted system's Master Boot Records (MBR), partition tables and other random data files. This caused the systems to become unusable [1].

VI. Security Solutions for ICS

Multiple security counter measures has been designed for ICS following the defense in depth concept and taking into account all ICS constraints of reliability and real time responses.in the following we discuss most relevant solutions during the different steps of security system lifecycle , starting by standards for securing ICS dependable systems as a requirement definition steps, security solutions for network protection as well key management systems for the design of authentication, authorization and integrity management.

1. Standards and guidelines

a. NIST Guidelines:

National institute of standards and technology (NIST) started a project on security of industrial control systems with applying NIST SP8053 [17] in Industrial control system. The aim of this project was the appliance of Federal Information Processing Standards (FIPS) [18][19] to industrial control systems as part of the federal systems. FIPS 199 and FIPS 200 require the following security controls for Federal systems: Access control, Awareness and training, audit and accountability, security assessment, configuration management, Identification and Authentication as well as Incident response. These requirements were introduces in specific publication for security in industrial control systems NIST 800-82 [1]. *NIST guide to industrial control systems security* provides typical ICS architectures and topologies, then discuss main threats and vulnerabilities of these systems.

The document provides also security countermeasures to mitigate the risk associated to the ICS vulnerabilities and threats. Authors propose a complete process to apply security in ICS starting by security policies and people awareness and following by conducting risk assessment for the ICS then apply security controls illustrated in the document. By far NIST 800-82 was the most detailed and specific guideline to secure industrial control systems for security owners.

The only limitation in the specification is the miss of design guidelines for ICS providers and vendors.

In February 2014, NIST came with a security framework titled; *NIST Cyber Security Framework* [20], the framework is providing a full process to implement cyber security from an organizational and technical point of view. *Identify, Protect, Detect, respond* and *Recover* are the five functions that the framework in proposing to ensure the cyber-security of a critical infrastructure. The five functions are referring to different standards such as IEC62443 [21], ISO27001 [22].

b. IEC 62443:

IEC 62443 formally called ISA99 Industrial *Automation and Control Systems (IACS) Security*; its aim is to create guidance documents on how to apply IT security in Industrial control systems including Hardware and software systems such as SCADA, DCS, PLC, HMI, networked sensors and devices. IEC 62443 is categorized into four main requirement categories; General requirements, Policies and procedures requirements, System requirements and Component requirements. *IEC62443* is the first standard that details requirements from system point of view by introducing in *IEC62443.3.x* [21] *Security Assurance Levels (SALs)* for industrial control systems and for specific security controls to implement for each SAL. Security assurance levels are assessed for each functional zone using seven functional requirements; Identification and authentication control, Use control, Data integrity, Data confidentiality, Restricted data flow, Timely response to event, Resource availability. *IEC62443.3.x* series are adopted by most of ICS vendors.

c. IEC 62351:

IEC 62351 is a recent standard developed by IEC for security in power system control operations. *IEC 62351* is an 11 parts Standard that covers all security aspects in power utilities communication. Part 1 and 2 are technical specification discussing security issues in power control systems. Part 4, 5, 6 are published as technical specifications o how to implement security in power control communication protocols, such as MMS, IEC61850 over TCP/IP. In addition to the security standard for communication protocols, IEC62351 Parts 7-11 are entailing larger scope to cover end to end security, involving security policies, access control mechanisms, key management, audit log, and other critical infrastructure protection issues [23].

2. Intrusion Detection and Prevention systems

Since ICS are using tailored protocols such as DNP3 and Modbus for real time and reliability purposes, the traditional IDS and IPS from the IT world don't answer the need of malicious events monitoring in the ICS. Therefore, new detection rules and monitoring mechanisms have been created specifically for ICS systems and networks taking into account the design specification of Communication protocols. The new rules and mechanisms are mainly based on attack signatures, anomaly detection, probabilistic models, system specifications as well as the behavior of ICS components [25][28].many research works have been done in this field to customize the IDS/IPS for the ICS focusing on the definition of new detection models relying on the protocols specification.[26][27]. The challenge related to the introduction of such techniques in the ICS is the difficulty of managing the distribution of IDS/IPS agents in all the system components and networks in a large scale system without decreasing the performances of the system. The other challenge that we see in the introduction of IDS/IPS into ICS is related to post detection reaction. Usually, when an intrusion attempt is detected, the targeted system is switched off and re-launched in a safe mode by reconfiguring the attacked parts. However, such reactions could not be applied to the ICS context as it could be used by an attacker to turn off the process as a reaction to a false positive intrusion.

3. Cryptographic counter measures:

All security objectives mentioned previously in section III and IV could be ensuring by using cryptographic techniques, which means the introductions off cryptographic algorithms in the ICS design in order to ensure the integrity and confidentiality of data in rest and in transit, authentication of messages origin and the message itself and non-repudiation of actions executed in the control system. The use of Cryptography counter measures in an ICS environment can be very costly in term of resources consumption. Another huge problem in the application of cryptographic techniques is the storage, distribution and renewal of cryptographic embedded in the control system components. Hence key management is a high priority for cryptographic system designer for ICS.

Key management is the process of controlling access to, and validating keys in a cryptographic system. Key management is primordial to ensure the right location and the validity of the key before using it for decryption [29]. Proper key management system is a whole set of operations including, key generation, randomization, safe storage with restricted access to unauthorized persons, key distribution, key update and the association of a key to an encrypted message exchanged between two or more communicators. Many researches has been done in this field in order to propose a key management system as an infrastructure for all cryptographic techniques required to ensure the security objectives in an ICS. In the following we give a literature overview on key management systems in ICS.

Key management systems for ICS

Two encryption methods families exist nowadays symmetric and asymmetric. Symmetric methods are relying on the fact the two communicators need to share the same key or tow somehow related keys to encrypt exchanged data. Which complicates the key management since for each pair of communicators, a different key is required. That implies the management of huge number of keys equal to the square of the system entities number. In the other hand, Asymmetric methods relies on the fact of using a pair of different but related keys for each entity known as public and private keys. To encrypt a message by A and send to B, A only needs the public key of B which is public [22]. In order to integrate those cryptography techniques into the ICS we cite in the following the different KMS for ICS.

Pietre-combacedes *et al* have introduced the main constraints for KMS in SCADA systems [33]. Based on these constraints, a high level survey has been done on the KMS which are based on four architectures; Key server based architecture, Point to Point architecture, a standard Public Key Infrastructure (PKI) as well as customized PKI. PKI based KMS has been included in the IEC 62351 standard as an infrastructure to build secure communications in power industry. The main issues in the KMS presented in this work are the scalability of the system and the freshness of the keys.

PKI based KMS should be considered but carefully due to the complexity of key renewals and certificate revocation and distribution issues in the distributed geographic areas [34]. Whereas symmetric key KMS are more attractive but more researches should refine customized KMS for ICS.

To address the scalability issue in key management solutions, Wong et al. [30] proposed the logical key hierarchy protocol, which based on the construction f a key tree from the leaves to the root, every node shares symmetric keys revised in every joining or leaving of node to /from the tree. The proposed key management scheme is scalable; however, the drawback of the scheme is that the keys secrecy is not guaranteed.

Choi *et al.* [31] proposed a key management scheme named Advanced Key Management Architecture (ASKMA) that supports message broadcasting and secure communications. The performance of the schema is relying on the minimization of processing load in the low power nodes. The scheme uses a logical key hierarchy. The scheme has many benefits; however, it may be less efficient during the multicast communication process. Another issue for ASKMA is its lack of availability.

Choi et al. [32] proposed ASKMA+, an improved and modified of ASKMA and is more efficient. This new scheme reduces the number of stored keys and provides efficient and protected multicast and broadcast communications. However, the availability issue of ASKMA+ is still not resolved.

All these previous works neglect the fact that ICS availability and real-time responses constraints should be the drivers of any KMS design for ICS including SCADA and DCS architectures. A good KMS in this case is the one requiring the use of minimum set of keys and with minimum exchanges between two nodes within the system.

VII. CONCLUSION AND PERSPECTIVES

This paper presents a deep overview on industrial control systems architectures, components and main protocols for a better understanding of the security issues in the ICS. We discussed the main security objectives and requirements for Industrial control systems and the differences between security in IT and security in ICS. Cyber attacks already discovered in the ICS raises the high requirement of deep investigation of security solution tailored for the industrial world. Standards as well as some research works are for the moment applying existing security countermeasures from the IT world on control systems. This could be useful but should be considered carefully since no customized security counter-measures for ICS exist today and the existing security solutions in IT have not been designed with the same constraints as the ones in ICS. The challenge for us and for all researchers in the ICS cyber security filed is to propose tailored security solution taking into account all the functional constraints of ICS. This challenge conducts us to review all the design of industrial control system components and communication protocols then redesign security mechanisms. In our future work, we will come with a proposal of customized key management system that supports the implementation of authentication and authorization mechanisms in ICS protocols and entities.

REFERENCES

[1] Keith Stoufler, Susan Lightman and Marshal Abrams:" Guide *to industrial control systems Security*" NIST special publication 800-82.May 2014.

[2] Stewart A.Boyer " SCADA: *Supervisory Control and Data Acquisition*" International Society of Automation 2009.

[3] Gregory K. McMillan "Process/Industrial Instruments and controls Handbook" McGrAW-HIL 1999.

[4] International Society of Automation: www.ISA.org

[5] North American Electric Reliability Corporation: http://www.nerc.com

[6] American Gas Association : www.AGA.org

[7] Erickson, Kelvin, and Hedrick, John, *Plant Wide Process Control*, Wiley & Sons, 1999

[8] Paul Didier, Reference Architectures for Industrial Automation and Control Systems, ODVA Industry Conference & 15th Annual Meeting October 2012

[9] Miller D, Byres E. Risk assessment: The first step. InTech 2005.

[10] Eric Knapp ,Industrial Network Security, MA ,2011

[11] M.J. Karam, F.A. Tobagi, Analysis of the delay and jitter of voice traffic over the Internet, in: Proc. of IEEE INFOCOM '01, 2001.

[12] P. Neumann, "Communication in industrial automation - what is going on?" in Control Engineering Practice. Elsevier Ltd, 2006, vol. 15, pp.1332–1347.

[13] M. S. Branicky, S. M. Phillips, and W. Zhang, "Stability of networked control systems: Explicit analysis of delay," in Proceedings of the American Control Conference. AACC, Jun 2000, pp. 2352–2357

[14] Dzung, D, Naedele, M, Von Hoff,T.P. Crevatin,M ,Security for Industrial Communication Systems, Proceedings Of The IEEE, Vol. 93, NO. 6, JUNE 2005.

[15] J. Viega and M. Messier, "Security is harder than you think," ACM Queue, vol. 2, pp. 60–65, Jul./Aug. 2004.

[16] Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Symantec 2014.

[17] Stuart Katzke and Keith Stouffer, Applying NIST SP 800-53 to Industrial Control Systems, ISO EXPO 2006

[18] Standards for Security Categorization of Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 199, February 2004.

[19] Minimum Security Requirements for Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 200, March 2006. Framework for Improving Critical Infrastructure Cybersecurity. NIST February 2014

[20] ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and SecurityLevels:

[21] ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels.

[22] W. Mao, Modern Cryptography: Theory and Practice. UpperSaddle River, NJ: Prentice-Hall, 2003.

[23] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, 2011, pp. 1-8.

[24] Zhu, Bonnie, and Shankar Sastry. "SCADA-specific intrusion detection/prevention systems: a survey and taxonomy." *Proc. of the 1st Workshop on Secure Control Systems (SCS)*. 2010.

[25] Cheung, Steven, et al. "Using model-based intrusion detection for SCADA networks." *Proceedings of the SCADA security scientific symposium*. Vol. 46. 2007.

[26] Tylman, Wojciech. "Native support for Modbus RTU protocol in Snort intrusion detection system." *New Results in Dependability & Comput. Syst. AISC* 224 (2013): 479-487.

[27] Goldenberg, Niv, and Avishai Wool. "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems." *International Journal of Critical Infrastructure Protection* 6.2 (2013): 63-75.

[28] Alohali, Bashar, Madjid Merabti, and Kashif Kifayat. "Key Management in Smart Grid: A Survey." *Proceedings of the PGNet* (2014).

[29] Sungjin Lee, Donghyun Choi, a. Choonsik Park, and S. Kim, "An Efficient Key Management Scheme for Secure SCADA Communication," *World Academy of Science, Engineering and Technology,* vol. 45, 2008.

[30] W. Chung Kei, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *Networking, IEEE/ACM Transactions on,* vol. 8, pp. 16-30, 2000.

[31] C. Donghyun, L. Sungjin, W. Dongho, and K. Seungjoo, "Efficient Secure Group Communications for SCADA," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 714-722, 2010.

[32] C. Donghyun, K. Hakman, W. Dongho, and K. Seungjoo, "Advanced Key-Management Architecture for Secure SCADA Communications," *Power Delivery, IEEE Transactions on,* vol. 24, pp. 1154-1163, 2009.

[33] L. Pietre-Cambacedes and P. Sitbon, "Cryptographic Key Management for SCADA Systems-Issues and Perspectives," in *Information Security and Assurance, 2008. ISA 2008. International Conference on*, 2008, pp. 156-161.

[34] Peisert, Sean, et al. "Control Systems Security from the Front Lines." *Security & Privacy, IEEE* 12.6 (2014): 55-58.