Era of Insecure Industrial Control Systems and Calamities to Come

Ashkan Sami, Abdullah, Khalili, Ali Davanian, Mahdi Azimi
Shiraz University
Shiraz, Iran
asami@ieee.org, akhalili@shirazu.ac.ir, {sina.davanian, mahdi1944}@gmail.com

***ABSTRACT*:** *Industrial control systems (ICS) control almost all the vital processes and industries that have direct effects on our lives. Recent information security breaches found in these systems have led to proliferation of attacks that can endanger not only the company they were deployed in but the people and environment around it. Stuxnet worm was a 'successful' story. Recently, it is shown that even regular attackers without sophisticated tools, like Stuxnet, can take control of ICS and create disasters. Even though vast amount of effort has put into securing ICS, this paper aims to illustrate that based on reported and experimentally obtained vulnerabilities on all aspects of ICS, no short term solution to protect ICS exists. This makes all ICSs vulnerable to at least one or more forms of attacks especially when network access is possible. Having insecure ICS will lead to dare consequences that will affect every one of us irrespective of color, nationality and religion. Since attack scenarios to ICS and code segments of malwares such as Stuxnet can be found on Internet, attacking ICS can be orchestrated with little effort from anywhere. Unfortunately, these forms of cyber attacks cannot be traced easily. The proven governmental investments to exploit these security breaches as untraceable weapons will lead the whole world into a very dark future. Last but not least, ICS with security considerations must be reinvented from the ground up and no patch can fix the problems if they not worsen it.*

Keywords: Industrial Control System, Security, SCADA Network, Industrial Protocols, Software

Received: 8 September 2013, Revised 12 October 2013, Accepted 17 October 2013

1. Introduction

Poisonous chemicals may spread over any city due to explosion in a nearby chemical company. Rotten meat due to disruptions in power lines will cause plague. Even water may be dispersed due to malfunctioning of distribution systems.Nuclear disasters more severe than Chernobyl are to come. All are due to security holes of industrial control systems that are the heart of industries mentioned above. Industrial Control Systems (ICS) like PLCs (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed control Systems) are the integral part of our industries. It is quite clear for control community that disruptions in normal operation of these systems can create disasters.This paper aims to illustrate different vulnerable aspects of ICS systems. An important fact that control engineers are not aware of is securing ICS (Industrial Control Systems), SCADA and etc. cannot be obtained by buying or adding "*Secure Products*" and tools. Actually, security cannot be implemented except by securing all devices and networks. In addition,since today's security mechanisms and tools to secure Information Systems (IS) do not guarantee a time response, use of these mechanisms and tools are not wise and cannot secure ICS.

Stuxnet is a highly sophisticated tool that consists of 14 different technologies [1]. Its '*success*' opened the door to a completely new form of war. Cybernetics now is a tool to create warfare.As any other kind of warfare,there must be counter

attack mechanisms to these new kinds of '*missiles*'. Unfortunately, it will be shown that technically no solution, method, tool or procedure can protect us from these cyber-attacks. In other words, with today's technology the heart of current industries industries cannot be secured into levels that keep '*knowledgeable*' attackers away.

In another successful attack scenario by an attacker with regular hacking tools to a PLC, it was shown that the attacker could execute unauthorized commands such as altering the messages sent to HMI, and taking control of the devices connected to the PLC [2]. The whole attack scenario was reported to Siemens; however, the developed patch was proven to be ineffective and the attacker again took control of the PLC [3]. The reason that Siemens cannot provide a '*bullet proof*' solution may be difficult for a control engineer to understand but for a security expert is easily understandable. Security is not an '*add-in*' feature and must be implemented in all parts of the system from design on.

This paper basically tries to illustrate no technologically feasible solution to secure current operational ICSs exist. In addition to reported vulnerabilities, experimentally obtained secure coding and architecture vulnerabilities of three open-source SCADA applications are illustrated as a proof of concept. Moreover, security problems of industrial protocols are also investigated.

Section 2 explains security principles and required controls. Section 3 highlights security priorities in contrast to control requirements priorities. Section 4 discusses problems in different parts of ICS. Discussion is presented in Section 5. Section 6 concludes the paper.

2. Security Principles and Required Controls

Principles are presented in a triad that can be called CIA which stands for *Confidentiality, Integrity and Availability* [4]. The terms are defined in Table 1.

Security principle	Definition
Confidentiality	States that critical information should stay secret and only those persons authorized to access it may receive access.
Integrity	Integrity is concerned with the trustworthiness, origin, completeness,and correctness of information as well as the prevention of improper or unauthorized modification of information [4].
Availability	Ensures information is readily accessible to authorized users. Although availability usually mentioned last, is not the least important pillar of information security [4].

Table 1. Information Security Principles

To achieve these principles, some controls are needed. The controls are shown but not limited to those illustrated in Table 2. These controls are used to maintain the triad of information security. For example identification, authentication, authorization and cryptography help to maintain information confidentiality and integrity.

3. Security Priorities in Contrast to Control Requirements Priorities

As said in the previous section, highest priority in information security is to maintain information confidentiality. Next priority is to maintain information integrity and the last is availability. However, for industrial control systems the order is exactly reverse. System availability is the most important requirement and integrity is the second highest. However, importance of confidentiality is low [5]. The contradiction between information security and control priorities is summarized in Table 3. It is clear that basic requirements for an information system significantly differ from ICS. This contradiction has led to proliferation of efforts to come up with solutions, tools, and technologies to meet the needs. As an illustration, Department of Homeland Security (DHS) has produced several documents on securing ICS. These documents are collection of suggestions, strategies and techniques to secure ICS [6]. However, proposed network security architecture is not built completely based on ICS requirement which will be discussed the next section.

Security principle	Definition
Authentication	Is the process of verifying the authenticity of detected identity
Authorization	Is a process which ensures that authenticated identities have rights to do requested operations.
Cryptography	Is the process of encrypting and decrypting of messages to make it confidential.
Accountability	Is the ability to trace performed actions and find their sources.
Identification	Is the process of uniquely identifying who is accessing the system.
Non-repudiation	Is a mechanism to ensure that a signed message is sent by the owner of signature.

Table 2. Security Controls

Security Principle	Information Security Priority	Control Priority
Confidentiality	High	Low
Integrity	High	Medium
Availability	Medium	Very High

Table 3. Priorities of Security Controls in Information Security and Control

In fact, any solution provided to secure ICS should meet following requirements [7]:

• Introduced latency must be minimal.

• It must support legacy systems.

• The technique must not cause safety implications.

• Cost should be reasonable.

• Solution must be fitted into existing telemetry environment without modification.

• Solution must be interfaced with standard bodies after the technology is proved.

These constraints limit security professional's abilities to secure ICS. In other words, meeting minimal latency and maximum security at the same time is highly demanding.

4. Security Problems in Different Parts of ICS

Security must be implemented in all devices that are in ICS. As stated earlier, security is not an add-in, but a framework that must be filled by practices and tools in all parts and segments of the system. If all parts of system are secured except one, that vulnerable point will be the entry point to the system.

Current solutions to secure ICS are divided into four categories: Equipments, Protocols, Software and Network security architecture. Even though availability is the most important factor in ICS and implementing these mechanisms should not jeopardize system availability, the solutions are provided without time limits and worst case scenarios.

4.1 Equipments

Equipments, in general, are all the devices used in control industries. These devices have considerable number of vulnerabilities. These vulnerabilities are mainly caused by lack of well-designed access control mechanisms. Access control includes identification, authentication, authorization and non-repudiation. In addition, such mechanisms decrease system availability. When access control mechanism has problems, taking control of the device is possible by exploiting the vulnerability. Vulnerabilities exist in devices produced by industrial companies like Siemens [8], General Electric [9],Schneider Electric [10] and WAGO I/O System 750 [11].

Due to page limitations, only vulnerabilities of Siemens products will be discussed in this section. Siemens PLCs have a very

severe vulnerability caused by hard-coded credentials. Hard-coded credentials are user IDs and passwords used for maintenance tasks. They are designed with this assumption that such devices cannot be accessed remotely but if attacker gains access to the device, knowing the hard-coded credentials leads to full control of the device [3].

Siemens PLCs S7-1200, S7-200, S7-300 and S7-400 also have non-repudiation mechanism vulnerability. This vulnerability makes the PLC susceptible to replay attack. Replay attacks are type of attacks that after recording a series of commands they can be resend and cause damage [12].

In contrast, to have a highly secure ICS, authentication and encryption must be incorporated at the same time. Since these mechanisms, especially encryption, requires processing time, they impose delay into the system. For instance, each time PLC is started, this mechanism needs user interference to enter the credentials. So process must wait until user enters the credentials.

4.2 Protocols

Industrial protocols have multiple types of vulnerabilities because they do not have some or all of the security controls. One reason is that adding security features jeopardize availability of the system. These intrinsic vulnerabilities in protocol design makes securing the communication channel very difficult and open the door to a set of attacks. In this section, some known attacks performed on industrial control will be discussed. An extended list of unimplemented security controls and corresponding attacks for popular industrial protocols is provided in 4.

It is important to note that safe and secure versions of some protocols exist but they are not widely used today. The problem is that old devices and software programs do not support these new versions. For example OpenSafety protocol which introduced in 2009 and commits to the IEC61784-3 supports all security controls [13]. Another example is secured CAN protocol which provides broadcast authentication [14]. As said earlier, migration to devices and systems which support these new protocols needs time. Thus, the problem of unsecured protocols still exists in most industrial systems.

For example, protocols like DNP3.0 or MODBUS have lots of these vulnerabilities [15] because they do not have any security controls as illustrated in Table 4. Note that currently many industries work with unsecure protocols. The cost of modifying current structure using secure version of protocols like Secure MODBUS and DNPSec is high.

In higher level protocols like OPC UA, non-repudiation mechanism is incorporated into protocol since it sits on the top of TCP/IP stack protocol. Thus, unlike field level protocols such as MODUS or DNP3.0, replay attacks are not easily orchestrated and sniffing or recording communication packets do not lead to meaningful attack scenario on OPC UA.However another severe attack called DoS (Denial of Service) can be orchestrated. DoS is a type of attack that system functionality or performance degrades significantly. Unfortunately DoS is one of the easiest attacks to organize. Stated differently, if an attacker sends a large number of packets to OPC UA server network card, server tries to respond to every packet. As a result it cannot respond to SCADA server commands on time [15]. For other protocols, similar attack scenarios can be designed.

A proposed solution to secure communication channel between sender and receiver may place a cryptographic module into both ends [16]. It cannot be a solution to all industries because security control mechanisms introduce latency that is incorporated with the security mechanism.

The other problem is a DoS attack scenario. Such modules must pass broadcast messages due to protocol specifications. Sending a lot of broadcast messages can form a Denial of Service (DoS) attack. Moreover, securing the channel having software applications like HMI and SCADA without security considerations in design time lead to exploiting the application via a secure channel.

Table 4 summarizes supported security controls by industrial protocols. The results are extracted from protocol specifications and verify that no security mechanism can secure the communication channel until the protocols are redesigned.

4.3 Industrial Software

Another problem even after securing only protocols is that secure channels may be used to exploit the vulnerabilities of industrial software programs. Industrial software has a lot of security problems. These problems are caused by secure coding problems and software architecture flaws observed in products from OPC client to SCADA and Datacenter servers [17].

	Profibus	Modbus	Modbus TCP	OPC	DNP3	HART	LonTalk	IEC	Industrial Ethernet	Attacks
Authentication	No	No	No	Yes	Yes	No	No	No	No	DoS, Unauthorized Command Execution, Data Poisoning
Authorization	No	No	No	Yes	No	No	No	No	No	Unauthorized Command Execution
Encryption	No	No	No	Yes	No	No	No	Yes	No	Sniffing
Identification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	DoS
Integrity	No	No	No	Yes	No	No	No	No	No	Man-in-the-Middle, Replay attack, Sniffing, Data Poisoning
Non repudiation	No	No	No	Yes	No	No	No	No	No	Spoofing, Replay Attacks, Data Poisoning

Table 4. List of industrial protocols, supported security controls and corresponding attacks

Category Name	Description
Critical Vulnerabilities	Dangerous vulnerabilities used by attackers. This category includes vulnerabilities like: • In-validated user input • Improper resource management • Buffer overflows • Improper access to memory
Vulnerabilities	Vulnerabilities that may be used by attackers but with less possibility than critical vulnerabilities. This category includes vulnerabilities like: • Weak cryptography • Improper exception handling
Bugs	These problems cannot be used by attackers but may lead the software to crash or unstable states: • Buffer overflows • Improper access to memory • Improper thread management • Improper resource management • Logical errors
Performance and Maintenance issues	These problems may decrease the availability of software or make the maintenance harder but their impact is low: • Unused codes and variables • Always true or false conditions • Non optimal functions

Table 5. Categories of secure coding problems

Secure coding includes techniques which prevent developers from producing problematic code [18].

Other types of problems are due to security problems in software architecture. Software architecture is the overall structure of application. Differences between software architectures are based on non-functional requirements such as availability,reliability, response time, and security. Software architecture for secure applications is in direct contrast to highly available applications. Software availability is improved using redundancy techniques in software architecture [19]. Redundancy techniques increase connectivity between modules. In contrast, security design patterns forbid redundancy and excessive connectivity. This architectural contradiction of security and reliability is due to the fact that each module is designed differently and should be secured differently. This indicates that software cannot be highly available and secure with current techniques at the same time. In fact, new architectural patterns should be developed to have highly available and secured software.

Soft	Open SCADA	Category	#of Files With Problem	#of Files With Problem	#of Files With Problem	#of Files With Problem
Open SCADA	1416	Critical Vulnerabilities	209	1144	5.47	18.29%
		Vulnerabilities	259	526	2.03	18.29%
		Bugs	283	731	2.58	19.57%
		Performance and Maintenance issues	106	183	1.73	7.3%
Mango	628	Critical Vulnerabilities	157	379	2.41	25%
		Vulnerabilities	205	398	1.94	32.64%
		Bugs	161	503	3.12	25.64%
		Performance and Maintenance issues	58	109	1.88	17.4%
MNDACS	193	Critical Vulnerabilities	49	247	5.04	25.39%
		Vulnerabilities	43	117	2.72	22.28%
		Bugs	50	199	3.98	25.91%
		Performance and Maintenance issues	46	179	3.89	23.8%

Table 6. Number and % of Problems in three Open-source SCADA applications

In this section, vulnerabilities of three java based open source SCADA applications that are investigated by a group of five M.S. and a Ph.D. student is illustrated; these applications are MANGO, MNDACS and OpenSCADA. These vulnerabilities are mainly categorized based on Common Weakness Enumeration (CWE) database which reports guidelines and remediation strategies on secure coding in software code [20]. Table 5 describes the categories used in this paper based on priorities of ICS. This table shows that some categories contain similar problems. For example buffer overflow is included in both Critical Vulnerabilities and Bugs. The reason is that each problem has several types. For example, stack overflow and heap overflow are types of buffer overflow. Based on probability of exploitation, these types are included in corresponding categories; stack overflow is considered as a Critical vulnerability and heap overflow as a Bug.

Based on proposed categorization, security problems of SCADA applications are listed in Table 6.This table indicates that industrial applications have lots of security problems. Critical vulnerabilities, Vulnerabilities and Bugs are the most frequent and Performance and Maintenance issues are the least. Large number of Critical vulnerabilities, Vulnerabilities and Bugs indicate that secure coding guidelines are not considered in the development of industrial applications and the only promising point is small number of Performance and Maintenance issues. This large number of severe security problems can improvise availability of industrial application and open the entry points to ICS.

These types of vulnerabilities are also frequent in commercial applications. Reports show that software products from companies like Tecnomatix FactoryLink [21], Control Microsystems [22], ABB [23], GE Intelligent Platforms [24], Invensys [25], Digital Electronics [26] and WellinTech [27] have these security problems also.

For example logging function of a windows service called CSService which is used by Siemens Tecnomatix FactoryLink application is vulnerable to a buffer overflow attack [21]. Buffer overflow can lead to take the control of host. This is an example of unsecure coding which proves that secure coding techniques is not considered mainly in industrial software development.

4.4 Network Security Architecture

Last but not least; network security architecture is an important aspect to secure ICS. Security architecture defines the structure of network – Sub-networks, Virtual Local Area Networks (VLANs) and Zones. It specifies where security technologies

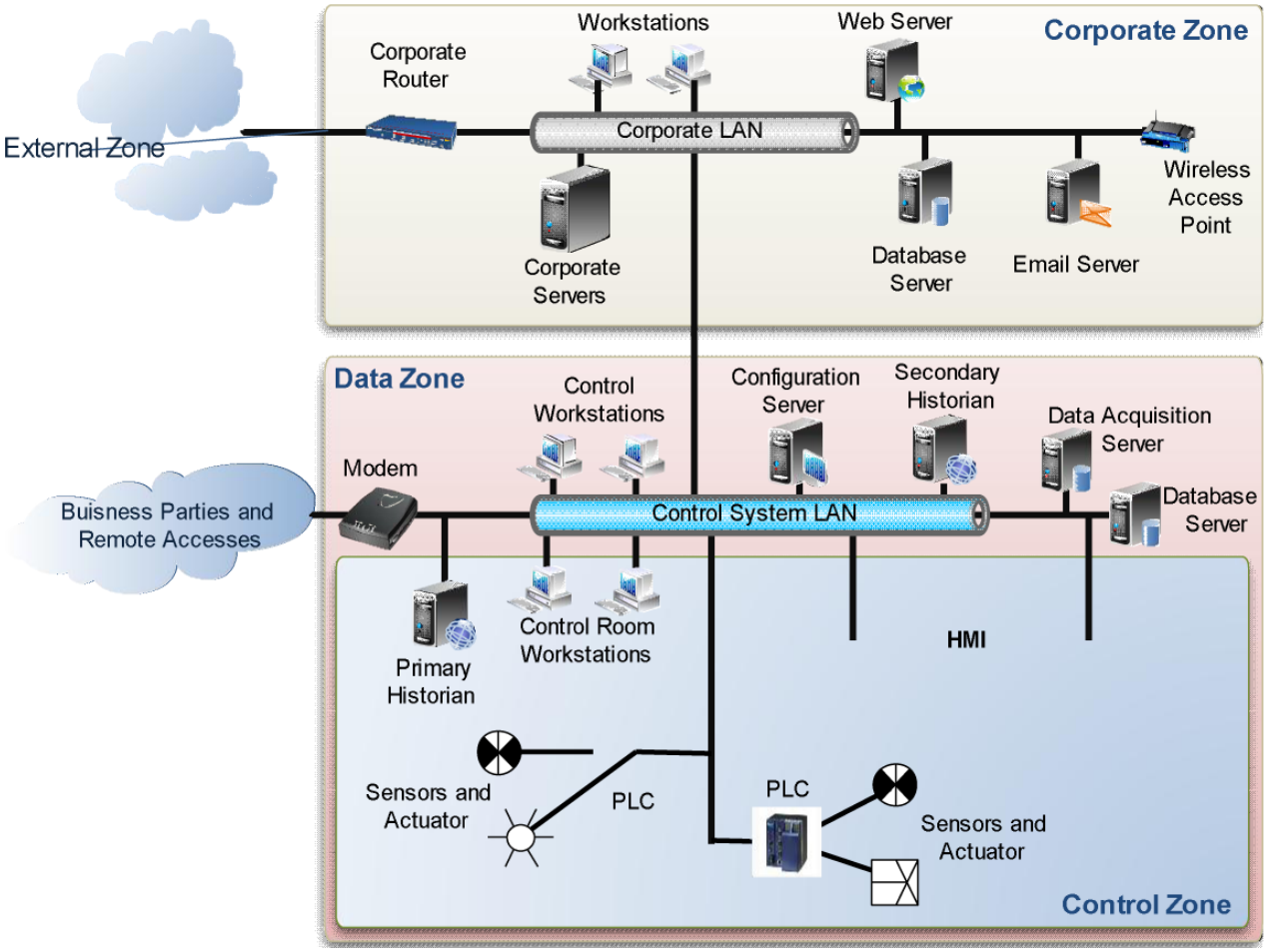

Figure 1. ICS zones

like firewalls, Intrusion Detection System (IDS), Security Information Event Management (SIEM) and other devices should be placed. Also, it specifies how they are connected together.

One of the first strategies to secure ICS is defense in depth strategy proposed by Department of Homeland Security (DHS) [5]. Even though defense in depth has several aspects, network security architecture is discussed here. In this strategy, ICS network is divided into four zones: External zone, Corporate zone, Data zone and finally Control zone. The zones are illustrated in Figure 1. External zone is Internet and any other area which is physically apart from internal LAN. Email servers, DNS servers and other business infrastructure servers reside in corporate zone. Data zone consists of historian and data acquisition servers which monitor and manage the control zone. Field devices and control room stations are in control zone.DHS proposed devices like firewall, System Information Event Management (SIEM) and Intrusion Detection Systems (IDS) to secure ICS. Proposed architecture is illustrated in Figure 2. As it can be seen, each zone is protected from other zones using firewalls, IDS and SIEM. Despite that, SIEM and Intrusion Detection Systems (IDS) monitor the traffic and detect attacks. In addition, SIEM responds to detected events. Access from external to internal zone is restricted through methods such as VPN connections. Un-trusted traffic such as wireless is encrypted. In each zone, services to other zones are resided on public servers. These servers are isolated from other systems using Demilitarized Zone (DMZ). DMZ is a sub network which restricts external accesses to these public servers.

As said earlier, information confidentiality is more important than availability in modern information networks [5] so sacrificing availability is reasonable. But for industrial control systems this is not the case because availability cannot be sacrificed.Proposed strategy of Defense in depth by DHS although states the importance of availability in the documents;however, no mechanism to guarantee tolerable latency is presented. Ignoring this fact makes all the proposals inappropriate for securing ICS. For example, placing firewall, IDS and SIEM introduces remarkable latencies. This is even

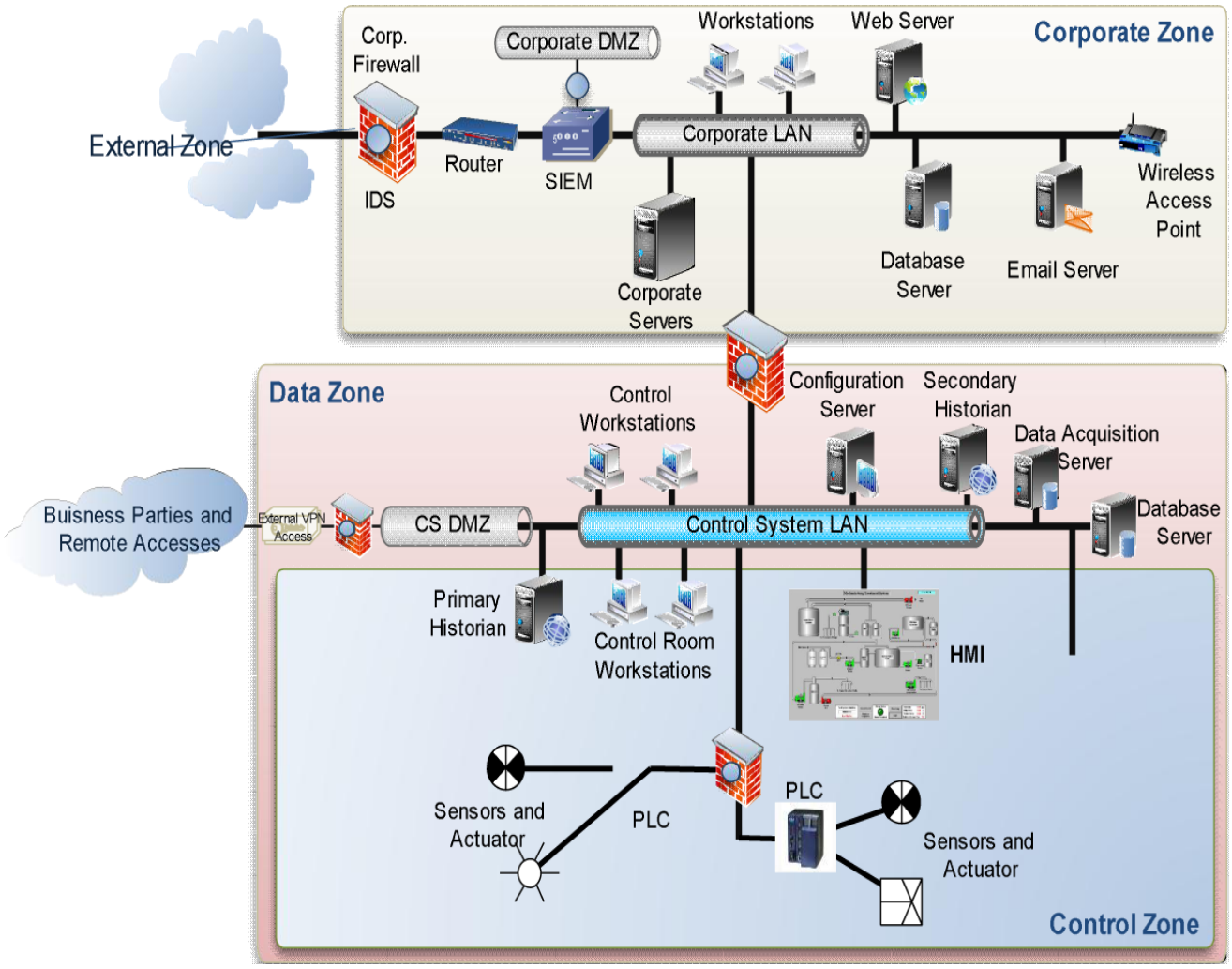

Figure 2. ICS Zones and Defense in Depth Strategy Using Security Devices

worse for the field level firewalls because latency is not tolerable. Moreover, using protocols like PROFIBUS in this zone exaggerates the problem because their transmission speed is slow and at most 1.5 Mb/s [28] so adding an encryption mechanism shall impose intolerable latency.

5. Discussion and Related Works

Researchers tried to secure the ICS in recent years. To the best of our knowledge, Cardenas et al [29] is the first advanced work which enumerates the challenges of securing the Cyber Physical System (CPS). They enumerated the security defenses that information security and control theory can provide to make the CPS survivable. They also enumerated a set of challenges that should be addressed to improve the survivability of CPS. The first challenge is to develop trust and adversaries models to better detect and categorize the cyber attacks. Second challenge is to design proactive algorithms to prevent the attacks based on adversary models. The most important issue that such algorithms must satisfy is the operational performance. Third challenge is to design reactive algorithms for real-time detection and response to the attacks. Finally, the last challenge is to assess the performance of physical system when attacks are done. Even though enumerated challenges help security experts to better understand the problem of securing ICS, no technical solution or guideline is provided.

Lin et al developed a framework to optimize the security for real-time systems [30]. They addressed the security requirements like confidentiality, privacy and authentication using a group-based security scheme. Each group contains several services with different security quality and overhead. Based on the framework, each group provides a security control. The problem is to choose optimized solution which satisfies required security quality and performance criterion with minimum possible overhead. Although provided results show that Integer Linear programming (ILP) could efficiently solve the problem, no technique or reference is provided to measure the quality of security services.

Cheminod et al developed a formal method to secure the communication channels and prevent the replay attacks [31]. The main contribution of their work is to develop a formal representation of communication protocols. Using the formal structure, efficacy of encryption algorithms can be evaluated in different abstraction levels. The disadvantage of proposed method is that formal methods are not scalable and sometimes applicable to secure all parts of ICS.

Similar works were done in [32]-[38]. All developed tools, techniques and methods addressed one or several security principals and dimensions but the main problem is that none of the methods considered the main difference between ICS and IT systems. In other words, researchers tried to make a tradeoff between security and operational performance. However,they all neglected that availability is not just a dimension of operational performance but the most important security principal in ICS. In fact, they used the approaches similar to IT systems to resolve the security problems in ICS. These approaches improve two sides of the security pyramid (confidentiality and integrity) but degrade the availability. The reason is that DoS is the most dangerous attack and easiest to orchestrate in industrial networks which jeopardizes the system functionality and ultimately disables the system. In summary, all proposed solutions did not envisage a counter-attack mechanism for DoS attack. Thus DoS attacks may be orchestrated with less effort. This states that security is not an add-in feature which can be added into the ICS structure. For example, in [34], a model is presented to solve the problem of security and availability tradeoff. The problem is that the model only takes the bandwidth as availability measure while memory and processing power usage that are ignored may play more crucial roles. Another problem with the presented solution is the assumption made in the paper. For example, if that tolerable overhead of encryption algorithm is less than 1 millisecond then the encryption key is less than or equal to 128 bits. Since Advance Encryption Algorithm (AES) with keys up to 128 bits can be broken, confidentiality is not improved while availability is also degraded.

As stated in the previous sections, computer security principals are not implemented into ICS. Security is not an add-in feature. Since in the construction phases of ICS, security was not the priority, patches cannot fix the problem and can be overcome. Known to all security experts, the regular and even advance solutions by security experts and the vendors to a vulnerable systemare not a remedy but also a cause of other exploitation and sometimes more powerful attacks. Conflicting requirements and conflicting architectures that are needed to guarantee security and availability make all the current technology and tools of information security inappropriate for securing ICS. The tools and mechanisms for securing ICS must be re-invented from the ground-up.

It takes a long time to invent and develop secure ICS tools and mechanisms. However, huge governmental expenditures on development of worms like Stuxnet and attackers with regular hacking skills in a setting that almost all of our industries are using insecure ICS, may not give us the required time to change current ICS with secured ICS that must be developed after a long development time.

6. Conclusion

It was illustrated that securing ICS into a level that regular attackers are incapable of taking control of ICS is almost impossible job with the current setting and technology used for information security. Experimentally obtained and reported vulnerabilities illustrated that almost all aspects of ICS contain security problems.Exploiting these vulnerabilities can cause potent implications. Having no solutions requires us to re-invent the mechanisms and tools to secure ICS from the ground-up.However, potential implications that exploiting vulnerabilities of current ICS provide has led to huge governmental investments to develop technologies for breaking ICS that is fragile by itself. The technology cannot be controlled and will affect us all.

References

[1] Fallier, N., Morchu, L. O., Chien, E. (2011). W32.Stuxnet Dossier, Ver 1.4, Feb, [Accessed: 13 July 2012].

[2] ICS-ALERT-11-161-01—Siemens Simatic S7-1200 PLC vulnerabilities, 10 June 2011, http://www.uscert.gov/control_systems/pdf/ ICS-ALERT-11-161-01.pdf, [Accessed: 13 July 2012].

[3] Bressford, D. (2011). Exploiting Norton Simatic S7 PLCs, NSS labs, July, [Accessed: 13 July 2012].

[4] Fundamental Security Concepts. http://www.mhprofessional.com/downloads/products/0072254238/0072254238_ch01.pdf, [Accessed: 10 July 2012].

[5] Department of Homeland Security Report. (2009). Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies, Control Systems Security Program, National Cyber Security Division, USA Homeland Security October.

[6] DHS recommended practices website. (2012). http://www.us-cert.gov/control_systems/practices/, [Accessed: 13 July].

[7] The Role of Authenticated Communications for Electric Power Distribution, Pacific Northwest National Laboratory, U.S. Department of Energy, 8-9 Novemeber 2006, http://www.truststc.org/scada/papers/paper34.pdf, [Accessed: 13 June 2012].

[8] ICSA-11-223-01—A summary of reported issues affecting Siemens Simatic PLCS, 11 August 2011, http://www.uscert.gov/control_systems/pdf/ICSA-11-223-01.pdf, [Accessed: 7 July 2012].

[9] ICS-ALERT-12-019-01A—GE d20me plc multiple vulnerabilities, 19 January 2012, http://www.uscert.gov/control_systems/pdf/ICS-ALERT-12-019-01A.pdf, [Accessed: 13 July 2012].

[10] ICS-ALERT-12-020-03B—Schneider electric Modicon quantum multiple vulnerabilities, 9 April 2012, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-020-03B.pdf, [Accessed: 13 July 2012].

[11] ICS-ALERT-12-020-07A—WAGO I/O 750 MULTIPLE VULNERABILITIES, 9 April 2012, http://www.uscert.gov/control_systems/pdf/ ICS-ALERT-12-020-07A.pdf, [Accessed: 13 July 2012].

[12] ICS-ALERT-11-186-01— Password protection vulnerability in Siemens Simatic controllers S7-200, S7-300, S7-400, AND S7-1200, 5 July 2011, http://www.us-cert.gov/control_systems/pdf/ ICS-ALERT-11-186-01.pdf, [Accessed: 13 July 2012].

[13]IECApproves OpenSAFETY, Bus-Independent Protocol. (2013). http://www.controleng.com/index.php?id =483&cHash=081010&tx_ttnews%5Btt_news%5D =36903, [Accessed: 20 June 2013].

[14] Groza, B., Murvey, S. (2013). Efficient protocols for secure broadcast in Controller Area Networks, IEEE Transactions on Industrial Informatics, Issue. 99, January.

[15] Fovino, I. N., Coletta, A., Masera, M. (2012). Security Technology Assessment (STA) Unit - Security of Critical Networked Infrastructures (SCNI) Action, Taxonomy of security solutions for the SCADA sector, 09 March 2012.

[16] Wang, Y., Chu, B.-T. (2004), SCADA: Securing SCADA infrastructure communications, Cryptology ePrint Archive, Report 2004/265, http: //eprint.iacr.org/2004/265.pdf.

[17] ICS-ALERT-11-230-01— Gleg agora scada + exploit pack update 1.4, 18 August 2011, http:// www.uscert.gov/control_systems/pdf/ICS-ALERT-11-230-01.pdf, [Accessed: 7 July 2012].

[18] Secure Coding. (2011). https://buildsecurityin.us-cert.gov/swa/downloads/Secure_Coding_v1.1.pdf, A software Assurance Pocket Guide Series, 6 (1.1), February.

[19] Yi, R. (2011). High Availability and Software Architecture, Master of Science Thesis, McMaster University, April.

[20] Common Weakness Enumeration (CWE), http://cwe.mitre.org/, [Accessed: 15 June 2013].

[21] ICS-ALERT-11-080-01-Multiple Vulnerabilities in Siemens Tecnomatics Factorylink, 21 March 2011, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-080-01.pdf, [Accessed: 10 July 2012].

[22] ICSA-11-173-01—CLEARSCADA remote authentication bypass, 25 August 2011, http://www.uscert.gov/control_systems/pdf/ICSA-11-173-01.pdf, [Accessed: 13 July 2012].

[23] ICSA-12-095-01—ABB multiple components buffer overflow, 10 April 2012, http://www.uscert.gov/control_systems/pdf/ICSA-12-095-01.pdf, [Accessed: 13 July 2012].

[24] ICSA-12-131-02—GE intelligent platforms proficy html help vulnerabilities, 27 June 2012, http://www.uscert.gov/control_systems/pdf/ICSA-12-131-02.pdf, [Accessed: 13 July 2012].

[25] ICSA-12-171-01—Wonderware suitelink unallocated unicode string vulnerability, 19 June 2012, http://www.uscert.gov/control_systems/pdf/ICSA-12-171-01.pdf, [Accessed: 13 July 2012].

[26] ICSA-12-179-01—Pro-face pro-server ex multiple vulnerabilities, 27 June 2012, http://www.uscert.gov/control_systems/pdf/ ICSA-12-179-01.pdf, [Accessed: 13 July 2012].

[27] ICSA-12-185-01—Wellintech kingview and kinghistorian multiple vulnerabilities, 3 July 2012, http://www.uscert.gov/control_systems/pdf/ICSA-12-185-01.pdf, [Accessed: 13 July 2012].

[28] PROFIBUS specification, March 98, http://www.kuebler.com/ PDFs/Feldbus_Multiturn/specification_DP.pdf, 2, [Accessed: 7 June 2012].

[29] Cardenas, A. A., Amin, S., Sastry, S. (2008). Secure control: towards survivable cyber-physical systems, *In*: Proceedings of the First International Workshop on Cyber-Physical Systems. (June 2008).

[30] Lin, M., Xu, L., Yang, LT. (2009). Static security optimization for real-time systems, IEEE Transactions on Industrial Informatics, 5 (1) 22–37.

[31] Cheminod, M., Pironti, A., Sisto, R. Formal vulnerability analysis of a security system for remote fieldbus access, IEEE Transaction on Industrial Informatics, 7 (1) 30 – 40, Feb.

[32] Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Fovino, I. N., Trombetta, A. (2011). A multidimensional critical state analysis for detecting intrusions in scada systems, IEEE Transactions on Industrial Informatics, 7 (2) 179-186, May.

[33] Zeng, W., Chow, M. (2011). A trade-off model for performance and security in secured networked control systems,IEEE International Symposium on Industrial Electronics (ISIE), June, p. 27-30.

[34] Fovino, I. N., Coletta, AA., Carcano, Masera, M. Critical State-Based Filtering System for Securing SCADANetwork Protocols, IEEE Transactions on Industrial Electronics, 59 (10) 3943-3950, October.

[35] Zeng, W., Chow, W. (2012). Optimal tradeoff between performance and security in networked control systems based on co-evolutionary algorithms, IEEE transactions on Industrial Electronics, 59 (7), July, p. 3016-3025.

[36] Fawzi, H., Tabuada, P., Diggavi, S. (2012). Secure estimation and control for cyber-physical systems under adversarial attacks, Cornell University Library, [Submitted:22 May 2012].

[37] Zeng, W., Chow, M. (2013). Modeling and Optimizing the Performance-Security Tradeoff on D-NCS Using the Coevolutionary Paradigm, IEEE Transactions on Industrial Informatics, 9 (1), February, p. 394-402.

[38] Cheminod, M., Durante, L., Valenzano, A. (2013). Review of Security Issues in Industrial Networks, IEEE Transactions on Industrial Informatics, 9 (1), February, p. 277-293.