Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring

Eugene Babeshko Vyacheslav Kharchenko Anatoliy Gorbenko

Abstract

Dependability and security analysis of the industrial control computer-based systems (ICS) is an open problem. ICS is a complex system that as a rule consists of two levels – supervisory control and data acquisition (SCADA) and programmable logic controllers (PLC) and has vulnerabilities on both levels. This paper presents results of the SCADA-based ICS dependability and security analysis using a modification of standardized FMEA (Failure Modes and Effects Analysis)-technique. The technique mentioned takes into account possible intrusions and is called F(I)MEA (Failure (Intrusion) Modes and Effects Analysis). F(I)MEA-technique is applied for determining the weakest parts of ICS and the required means of fault prevention, fault detection and fault-tolerance ensuring. An example of F(I)MEA-technique applying for SCADA vulnerabilities analysis is provided. The solutions of SCADA-based ICS dependability improvement are proposed.

1. Introduction

The current security and safety level of SCADA-based systems does not correspond to the possible threat consequences. There is a large quantity of implemented industrial control systems which are relatively insecure and unsafe due to different kinds of disclosed vulnerabilities. Arbitrary applications of technology, informal security, and the fluid vulnerability environment lead to unacceptable risk [1]. Any vulnerability can lead to a failure if an intrusion occurs.

To improve dependability of SCADA-based systems and ensure their fault and intrusion tolerance, it is necessary to take into account the majority of possible failure and intrusion modes, their causes and the resulting influence on the system. With this purpose we propose to use a modification of standardized FMEA (Failure Modes and Effects Analysis)-technique [2] called F(I)MEA (Failure (Intrusion) Modes and Effects Analysis) [3]. In this paper we focus on analysis and ensuring reliability, security and safety of the SCADA-based industrial control systems.

The structure of the paper is organized as follows. Section 2 gives short description of SCADA-based industrial control systems, their typical architectures and functions. In Section 3 we present results of failure and intrusion modes and effects analysis of SCADA-based systems. In section 4 we give recommendations concerning dependability ensuring according to the results obtained. Finally, section 5 contains conclusions and briefly outlines the future work on implementation and reengineering of dependable and secure SCADA-based ICS.

978-0-7695-3179-3/08 $25.00 © 2008 IEEE
DOI 10.1109/DepCoS-RELCOMEX.2008.23

2. SCADA-based industrial control systems

Industrial control systems are extensively applied in different safety-critical infrastructures like electric power stations, oil, petroleum and natural gas communication, conversion and refinement, as well as in various manufacturing operations. Such systems are used to centrally monitor and control remote or local industrial equipment such as motors, valves, pumps, relays, sensors, etc. ICS are dependability (safety, reliability, security)-critical and critical to efficient operation of many physical processes.

Typical ICS consists of two levels – supervisory control and data acquisition (SCADA) and programmable logic controllers (PLC).

SCADA is a necessary element of the most modern ICS. We define ICS that includes SCADA as SCADA-based industrial control system. Typical elements of SCADA-based industrial control systems and its functions are shown in the Fig. 1

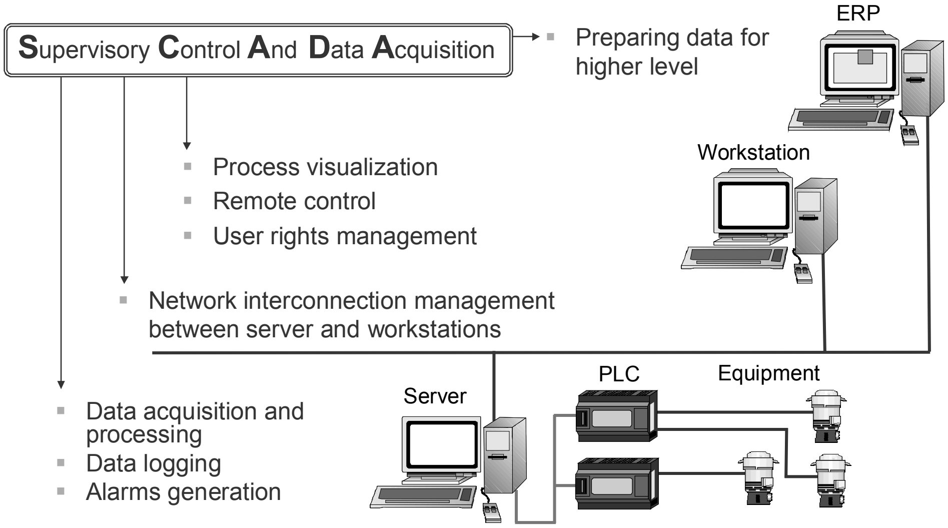
Supervisory Control And Data Acquisition
Preparing data for higher level
ERP
Workstation
Process visualization
Remote control
User rights management
Network interconnection management between server and workstations
PLC
Equipment
Server
Data acquisition and processing
Data logging
Alarms generation

Figure 1. Typical SCADA-based industrial control system

SCADA includes server (alarm server, data logging server, etc.), workstations and communication services. Server processes and logs data generates alarms, workstations provide Human–Machine Interface (HMI) to users, communication lines are used for data transmission between server, workstations and other equipment.

The SCADA network is usually connected to the outside corporate network (for example, to provide enterprise resource planning (ERP) systems with process information) and/or the Internet through specialized gateways [4]. Traditionally ICS were isolated and used proprietary control protocols with specialized hardware and software [5]. Modern systems use Internet protocol devices and share information with a large community (for example, [6]). Moreover, remote access to ICS via different communications channels, even wireless, is usually allowed for maintenance. This improves system usability but increases the risk of cyber intrusions. Generally, nowadays there is a tendency that SCADA-based systems improve their performance and convenience every year but their security is still in poor condition.

Proposed classification of SCADA-based ICS taking into account the problem of intrusion-tolerance is shown on the Fig. 2. In our opinion, designing systems and already implemented ones should be distinguished because analysis of designing systems can help to avoid vulnerabilities during the design stage. Performance of such an analysis for systems which are already in use is more complicated. Moreover, performing some operations on vulnerability elimination is not always possible because of uninterruptable operation manner of most ICS.

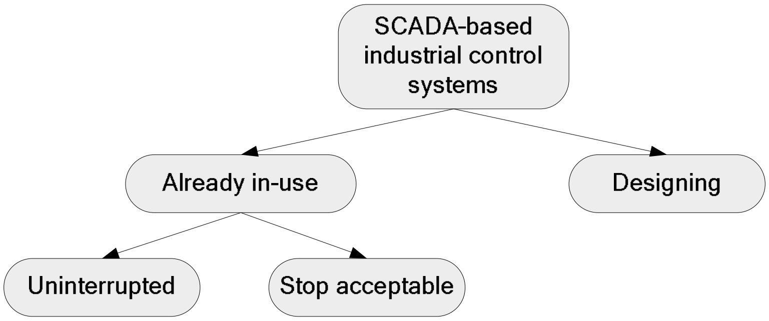

Figure 2. Classification of SCADA-based systems

Inadmissibility of SCADA-based system interruptions leads to difficulties in installing security patches that eliminate disclosured vulnerabilities. SCADA and other components like PLCs tend to be hard to upgrade. For example, PLC may use an operating system and application that were burned to ROM and which are not rewritable at all. Or, in case of relatively old systems, the PLC vendor may no longer be in business or may not be producing necessary upgrades.

Therefore, any part of SCADA-based system can be insecure. So, each element should be analyzed and, if it doesn't have necessary security level, it should be replaced with other element with the same functionality but with higher security level.

Any failure (caused physical, design or interaction faults) can lead to data loss. So all predicated failures should be prevented. How to understand which elements of SCADA-based systems are the weakest places? We propose F(I)MEA-technique for determining this.

3. F(I)MEA –technique for SCADA-based ICS analysis

3.1. An overview of F(I)MEA

The FMEA is a standard formalized technique for the systems reliability analysis devoted to the specification of failure modes, their sources, causes and influence on system operability [2]. "Failure modes" means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential (that can happen) or actual (that already happened). "Effects analysis" refers to studying the consequences of those failures.

In FMEA-technique, all possible failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. FMEA is used during the design stage with an aim to avoid failures in future. In the next stages it is used for process control, before and during ongoing operation of the process. The purpose of the FMEA is to take actions to eliminate or reduce possible failures, starting with the highest-priority ones. It also may be used to evaluate risk management priorities for mitigating known threat-vulnerabilities.

IMEA (Intrusion Modes and Effects Analysis) is a modification of FMEA that takes into account possible intrusions to the system [3].

Why do we use IMEA instead (or in addition to) a standardized FMEA? There are some reasons. First of all, SCADA-based industrial control systems as a rule are critical systems. Besides, they are quite reliable, but, nevertheless, like any complex systems, SCADA-based ICS have different vulnerabilities that can be used by an intruder. Any vulnerability can become a failure if an intrusion occurs. So we use IMEA to take into account failures caused by intrusions "using" system vulnerabilities.

It should be noted that FMEA and IMEA are not the only methods for complex systems failures and risks analysis. Different approaches are shown and examined in the work [7]. But we think that F(I)MEA technique is the most convenient and clear for specified task.

3.2. F(I)MEA tables for SCADA-based ICS

As it was said before, a SCADA-based system consists of hardware (PLCs, PCs, switches etc.) and several specific software components (database server, HMI clients, PLC program) and may have different architectures (Fig. 1). Each of these components should be taken into consideration during analysis of failure modes and effects.

In this article it is examined two levels of SCADA-based ICS – SCADA and PLC. We mark out data server (hardware and software), OPC server (software), HMI workstation (hardware and software) on SCADA level and discuss PLC hardware and PLC software on PLC level.

In our opinion, failure influences on system operability could be interruption, termination and no influence. Interruption means that one or several system functions are not performed correctly. For example, in some cases SCADA-based system failure may not directly cause the damage, but it may make it impossible for some businesses to operate. Termination means that system doesn't operate at all. In some cases, termination of a SCADA-based system causes serious problems, such as discharge of a pollutant, destruction of property, fatalities. Described taxonomy is shown on the Fig. 3.

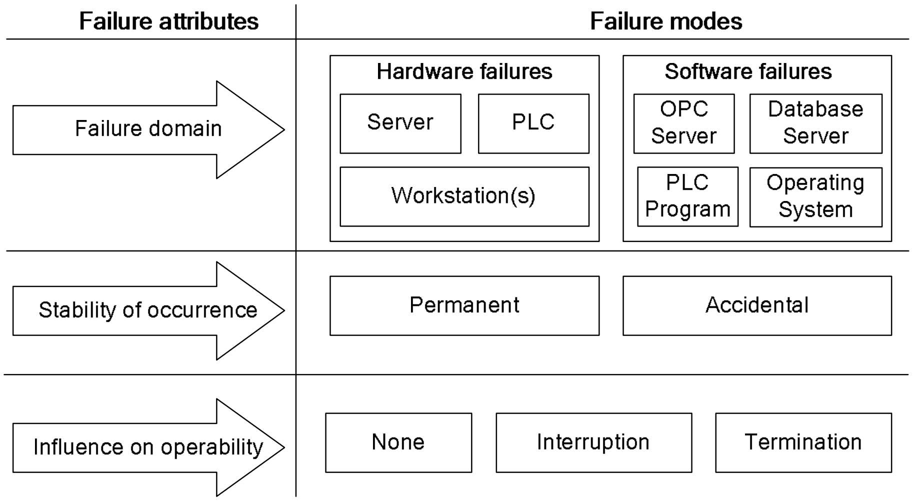

Figure 3. Failure mode taxonomy

We performed the analysis of failures and intrusions effects for software, hardware, stored data, users and SCADA-based system as a whole. As an example we took a real SCADA-based gas cleaning system that consisted of the server, 4 workstations and 3 PLCs [8]. Obtained results were generalized to present typical SCADA-based ICS analysis (see Tables 1-2).

Table 1. Failures modes and effects analysis

Failure Domain	Stability of Occurrence	Failure Cause	Influence on Operability	Failure Evidence	Failure effect				
					HW	SW	Stored data	SCADA-based system as a whole	User
HW environment	accidental failures	PLC halt	termination	evident	crash	crash	-	limited functionality	deny of service
			interruption	evident		suspension	-		deny of service
		workstation PC fault	termination	evident		crash	-	limited information about process state	deny of service
			interruption	evident		suspension	-		deny of service
		server PC fault	termination	evident		crash	data loss	no data logging, no information about process state	deny of service
			interruption	evident		suspension			deny of service
	permanent failures	design faults	termination	evident	-	-	-	incorrect operation	deny of service
			interruption	evident	-	-	-		deny of service
			-	non-evident	-	-	-		incorrect service
SW environment	accidental failures	incorrect input data	termination	evident	-	incorrect operation	-	incorrect operation	deny of service
			interruption	evident	-		-		
			-	non-evident	-		-		incorrect service
		malicious impact (intruder attack)	termination	evident	-		-		deny of service
			interruption	evident	-		-		
			-	non-evident	-		-		incorrect service
	permanent failures	design fault	termination	evident	hang	crash	corruption		deny of service
			interruption	evident	hang	suspension	-		
			-	non-evident	hang	incorrect operation	-		incorrect service

Table 2. Intrusions modes and effects analysis

Intrusion/Attack mode	Attack nature	Attack Cause	Influence on Operability	Intrusion Evidence	Intrusion effect				
					HW	SW	Stored data	SCADA-based system as a whole	User
Sniffing	passive/ active	sharing information with large community	termination	non-evident	-	-	privacy violation	SCADA-based system compromise	unauthorized access to user's data
			interruption		-	-			
			-		-	-			
System remote control	active	weak authentication	termination	evident	-	-	privacy and integrity violation	SCADA-based system incorrect operation	deny of service
			interruption		-	-			
			-	non-evident	-	incorrect operation			
OPC buffer overflow	active	OPC server without latest security patches	termination	evident	-	crash		SCADA-based system termination	
			interruption		-				
			-		-				
DoS & DDoS	active	weak system protection	termination	evident	hang	crash			
			interruption						

4. Ensuring SCADA-based ICS dependability

4.1. Error recovery

Error recovery allows restoring a compromised system to its operational status. The main means of SCADA-based industrial control systems error recovery are:

1) replacement of crashed hardware modules;

2) reinstallation of crashed software components (SCADA level), redownloading software if possible (PLC level);

3) installation/downloading of patches that fix known errors (if acceptable);

4) restarting servers (database server etc.), restarting PLCs.

To achieve better level of ICS availability, it is necessary to have spare parts for SCADA-based ICS critical components. For example, if system has several PLCs that are hardware identical but have different software and different functions, at least one PLC must be available as a spare part.

4.2. Fault detection

SCADA-based ICS user should get alert or warning for any abnormal behaviors before process becomes out of control. When any fault is detected, the graphical display and alarm messages should be shown to help user in identifying the fault place and source. Modern PLCs and SCADA provide extensive diagnostics and standard SCADA means can be used for displaying and alarms generating.

4.3. Fault prevention

Fault prevention is the process of reducing the risk of an unwanted incident. This procedure uppermost is attained by quality control techniques employed during the design and manufacturing of hardware and software [9]. That is, the majority of effective fault prevention measures must be built into the SCADA-based ICS architecture and should not be added later. But for most critical systems it is impossible to foresee all possible faults. So fault prevention must be the part of regular system maintenance activities. Examples of fault prevention actions are:

1) checking of input parameters for acceptability both on SCADA and PLC levels. Even if incorrect input data was transferred to PLC (as a result of SCADA design error, or as a result of an intrusion), PLC should not produce incorrect actions. Only an appropriate alarm should be generated;

2) minimization of corporate network and industrial network interconnections. The most preferable choice is a complete SCADA-based ICS isolation from a corporate network;

3) implementation of security checking on all levels of SCADA-based ICS. User authorization and permissions must be configured properly. Workstations and servers operating systems should not have default accounts and simple passwords;

4) data encryption;

5) removing and closing all unused ports and services.

5. Conclusions

Dependability analysis of SCADA-based industrial control systems should be performed not only during the design stage, but during system operation as well. New vulnerabilities are discovered very often and much attention must be paid to react to them. Taking into account this circumstance, SCADA-based ICS should be evolvable systems, i.e. they should be able to evolve according to challenges related to changes of intrusion environment.

The F(I)MEA is one of the most convenient techniques for SCADA-based ICS dependability analysis. FMEA and IMEA tables clearly represent current vulnerabilities and possible failures of SCADA-based systems. These tables are the base for the next step of dependability assessment using, for example, PSA- or FTA-techniques.

Results of F(I)MEA-analysis may be detailed depending on type and features of SCADA-based ICS. More detailed and thorough analysis allows developing, fitting and implementing more efficient means of dependability ensuring.

6. References

[1] Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, William Young. “Sustainable Security for Infrastructure SCADA” [Online]. Available: http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf

[2] IEC 812. Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA). International Electrotechnical Commission, Geneva (1985)

[3] Anatoliy Gorbenko, Vyacheslav Kharchenko, Olga Tarasyuk, Alexey Furmanov. “F(I)MEA-technique of Web Services Analysis and Dependability Ensuring”, *Lecture Notes in Computer Science*, vol. 4157/2006, pp. 153-167

[4] Vinay M. Igure, Sean A. Laughter, Ronald D. Williams. “Security issues in SCADA networks”, *Computers & Security*, № 25 (2006) pp. 498 – 506

[5] Stouffer K., Falco J., Kent K. “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. Recommendations of the National Institute of Standards and Technology” [Online]. Available: http://csrc.nist.gov/publications/

[6] Kato M., Watahiki K., Suzuki T. “Integration of Supervisory Control and Data Acquisition Systems Connected to Wide Area Networks”, *Hitachi Review,* Vol. 53 (2004), No. 3, pp. 169-173

[7] White D. “Application of systems thinking to risk management: a review of the literature”, *Management Decision*, 1995, vol. 33, № 10, pp. 35-45

[8] Eugene Babeshko, Vyacheslav Kharchenko. Gas cleaning system dependability assessment. *The second international scientific and technical conference "Dependable systems, services and technologies" (DeSSerT).* Kirovograd, Ukraine, 2007

[9] Avizienis A., Laprie J.-C., Randell B., Landwehr C. “Basic Concepts and Taxonomy of Dependable and Secure Computing”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 1(1) (2004), pp. 11–33