Safety vs. Security in Industrial Control

Andrew J. Kornecki
Electrical, Computer, Software & System Eng.
Embry Riddle Aeronautical University
Daytona Beach, FL 32114
1-386-226-6888
kornecka@erau.edu

Janusz Zalewski
Computer Science
Florida Gulf State University
Ft. Myers, FL 33965
1-239-590-7317
zalewski@fgcu.edu

ABSTRACT

In this paper, we present a view on the system security, which draws from the previous experiences in dealing with system safety. Both issues are treated as mutually complementary views of the same problem: security as protecting a computer system against the threats of the external environment, and safety as protecting the environment from potential dangers of a computer system. Mutual relationships of safety and security are discussed.

Categories and Subject Descriptors

C.3 [**Computer Systems Organization**]: Special-purpose and Application-based Systems – *process control systems, real-time and embedded systems.*

D.2 [**Software Engineering**]: Requirements/Specification – *design, software architectures, interoperability.*

General Terms

Security, Standardization, Verification

Keywords

Industrial Control, Security, Safety, Software Assurance.

1. INTRODUCTION

Historically, industrial computer control systems were designed so that their operations would not compromise safety i.e. would not endanger the environment and people in terms of death, injury, or large financial losses. On the other hand, the security of industrial computer control systems was typically limited to physical plant access and off-line protection of data. With the miniaturization of computing devices, growing sophistication of control, and the proliferation of internet use, multiple functions of industrial control systems have become accessible online, opening doors to security threats. Due to the increasing role of software in the nation's critical infrastructure, there is a need to address software's impact on systems safety. Examples of industrial control systems requiring particular attention are the power grid, nuclear power stations, water and food plants, chemical factories, oil refineries, railway, and air traffic.

The recent tendency is to replace older federated and well protected discrete controls with new integrated complex digital systems that are not only interconnected in the control network but also connected with conventional, typically Ethernet-based access to the general computing network—for the purpose of remote control, data collection, monitoring, etc. Often developers of these new systems are not fully aware of the security issues that such new architectures may bring, and the IT professionals may neglect the need for additional safety precautions like analog/mechanical backup, etc. Control engineers may not be familiar with security issues like leaving open connections, retaining default passwords, and not keeping anti-virus software up to date. Thus, to increase assurance of industrial computer systems, security concerns have to be taken into account, and the mutual relationships of safety and security studied and reconciled.

2. BACKGROUND

Security of Industrial Control Systems (ICS) has been a known concern for some time. Dzong et al., in their overview of relevant issues [1], state that the reuse of open protocols in such systems "facilitates development and deployment of highly connected systems, but also makes the communication system vulnerable to electronic attacks." Stouffer et al. make a similar point [2] that "the trend towards integrating ICS systems with IT networks provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats." Identical trends are observed in embedded systems [3-5], where security issues have been recognized some time ago. Koopman, for example [3], states that "Security for embedded systems involves issues beyond those problems currently addressed for enterprise and desktop computing."

More recently, Parameswaran and Wolf [4] in their overview notice that "These devices are inherently vulnerable to many operational problems and intentional attacks due to their embedded nature." and Stammberger [5] confirms that "With millions of new electronic devices connecting to the Internet every day, hackers are increasingly focusing on a new type of target: mobile and embedded systems." Particular industries, for example, nuclear [6], automotive [7] and medical devices [8], to name a few, began addressing related issues individually. The importance of these issues became so crucial to the nation's economy and security that it resulted in holding congressional hearings [9-10]. D.A. Shea, in his Report for Congress [9], warns that "The potential consequence of a successful cyber-attack on critical infrastructure industrial control systems range from a temporary loss of service to catastrophic infrastructure failures affecting multiple states for an extended duration", and J.M. Weiss, in his testimony before the U.S. Senate [10], suggests that

"One should view ICS cyber security as where mainstream IT security was fifteen years ago – it is in the formative stage and needs support to leapfrog the previous IT learning curve."

Some peculiarities of control elements may cause problems. It has been reported in a congressional testimony [1] [10] that networked Programmable Logic Controllers (PLC) may fail when exposed to excessive network traffic. The cited case resulted in a scram and manual shutdown of Brown Ferry nuclear reactor following loss of both recirculation pumps due to a goof-up of IT technician that decided to ping all devices on the network - and PLC controlling the pumps were among of them. We need to note that regulated industries are using their guidance documents and standards when providing the software and hardware safety assurance arguments for their systems, and thus the base for systems certification.

3. PROBLEM AWARENESS

From the technical perspective, security cannot be treated in isolation from other quality attributes of computing systems such as safety, both being a part of overall system trustworthiness (Fig. 1). In industrial applications, with a control system in charge of the technological process, safety was typically considered a critical system property.

Symptomatically, the topic of addressing jointly safety and security of computing systems was covered in keynote addresses by speakers from industry at two recent professional conferences. At SAFECOMP2009, which is a long lasting International Conference on Computer Safety, Reliability and Security, and had its 28th edition in September 2009, the keynote talk [11] was delivered by Walt Boyes of Control Magazine (with 25 years of experience in industry), who discussed the problems of vulnerability of critical infrastructure due to the increasing interconnections with the external networks and the IT systems. The question posed is whether or not the safety system built on top of the control systems is not only safe but also secure. Boyes identified situations when security violations may lead to safety violation and thus related incidents resulting even in some fatalities. He observed that cyber security issues must be considered in any safety implementation in any process plant, just as safety issues must be considered when administering IT security issues.

At the second conference, WRTP2009, the 30th IFAC Workshop on Real-Time Programming, George Romanski, President of Verocel, Inc., a company dealing with hardware and software certification for the FAA, also touched on the issue of mutual relationships between safety and security in embedded systems used in Integrated Modular Avionics [12]. According to Romanski, due to the huge increase in processing power and memory available to the applications, the vulnerability of embedded computing systems – understood as threats to their safety and security – has significantly increased and needs to be constantly addressed in both aspects.

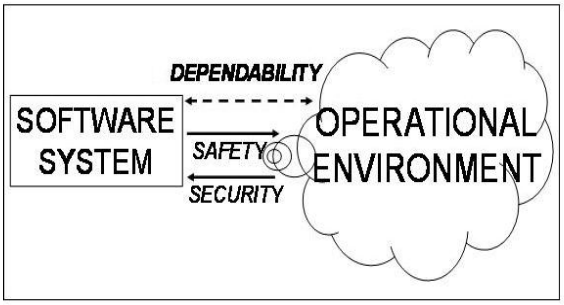

Figure 1. Illustration of Component Properties of System Trustworthiness.

Other examples of joint security and safety concerns can be given. The real question is: how much can we trust modern industrial control systems, which are interconnected with corporate management networks? This research will explore the concepts of functional safety and functional security - their relationships and methodology to increase the assurance for software intensive control systems in a contemporary network intensive environment.

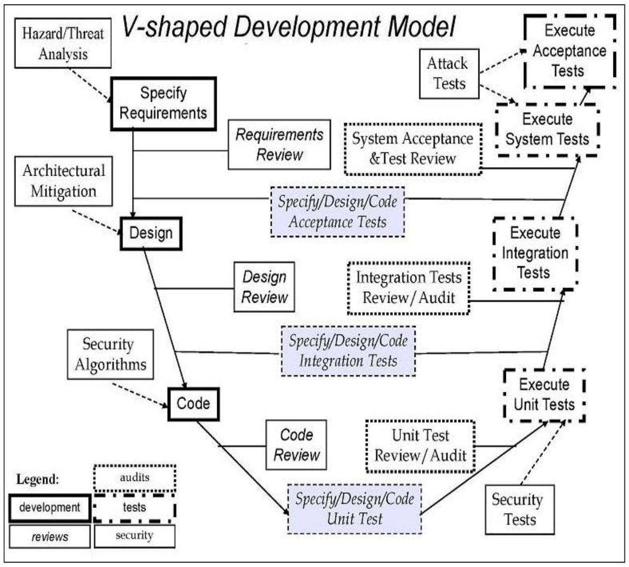

Figure 2. V-shaped Model with added Security Actions.

One of the most popular development models in embedded software is V-shaped (Figure 2). However, the conventional V model does not consider security. It is imperative for the systems that can be working in a networked and wireless configuration to add components reflecting necessary security actions:

- Hazard/threat analysis
- Architectural mitigation
- Security algorithms
- Security threats
- Attack tests

[1] http://www.controlglobal.com/industrynews/2007/168.html

How much can we trust industrial control systems interacting with enterprise networks? A trusted product is assumed correctly enforce its security functional requirements. We define trustworthiness as measure of the degree to believe something or that a certain phenomenon to be trusted. From perspective of security we define system access trustworthiness as a threshold which shows the least trustworthiness of the user who can log in or access the system and thus have impact on its operations. The value is taken as a decision condition to judge whether the user has passed authentication. The feedback from industry working on daily basis with such system is critical for problem understanding.

Safety analysis of a computer system starts with identifying potential hazards that may be caused by software or hardware failures or external conditions [13]. Analyzing software architecture is particularly helpful, in this respect, because it identifies the major components that may be potential sources of such hazards. Since security analysis originates by identifying potential threats/attacks, it is expected that techniques developed for safety analysis will be applicable for security assessment.

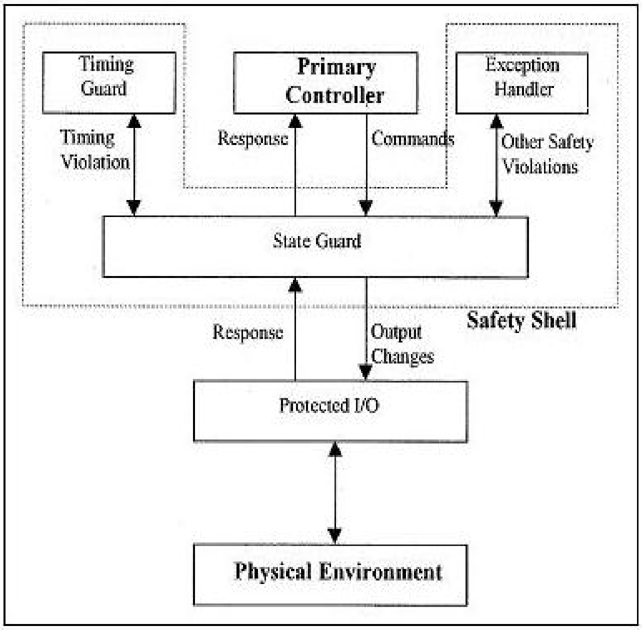

Figure 3. Safety Shell Architecture [19].

Even though there are multiple, well established methodologies and techniques to address safety concerns during the development process [13-14], they do not discuss safety and security as two related aspects of the same problem. The approach co-developed by one of the authors, under the name of safety shell, (Fig. 3) [15], which relies on an architectural model enabling design of control systems [16], shows a striking similarity to a typical "onion model" of security assurance. The concept is based on implementing a "test first" design element to prevent dangerous situations from occurring, which is meant to detect a hazardous situation at its beginning. By "testing first" the hardware processor or software shell will either validate or invalidate the current action and/or the desired action. The concept has been independently developed further to map the design on the UML model [17].

4. CHALLENGES AND SOLUTIONS

Koopman [3] asks several questions related specifically to embedded systems. How to create firewalls to keep attackers from manipulating safety-critical sensors and actuators? How to ensure meeting real-time deadlines during a denial-of-service attacks or when system components are compromised? Can intrusion-detection system respond fast enough to restore a system to correct operation before a control loop loses stability? Can unattended embedded systems be securely upgraded without being vulnerable to attacks on the upgrading mechanism? Can attacks designed to drain batteries be detected and avoided? Can all this be done on a $1 microcontroller?

These questions are symptomatic to the specific challenges facing modern industry. Analyzing issues of safety and security for industrial control system allows us to identify several challenges:

- Challenge 1: Industrial safety systems are not designed for security.
- Challenge 2: Typical intrusion-detection may not be an acceptable solution.
- Challenge 3: Wireless connection makes systems vulnerable to remote security intrusions.
- Challenge 4: Integration problems for systems that were previously operated separately.
- Challenge 5: IT personnel versed in security may not be familiar with industrial control requirements.
- Challenge 6: COTS components may allow for an easy access to unprotected systems.
- Challenge 7: Outsourcing may provide the overseas personnel to access domestic industrial networks.
- Challenge 8: Security-safety knowledge gap in education of software, computer, and system engineers.

To address these challenges the following actions are proposed:

- Analysis of the security threats from the perspective of industrial control systems.
- Design of a test-bed for testing selected threats.
- Investigation of potential countermeasures and mitigation mechanism.

From the implementation perspective, there are several options to increase industrial systems security assurance. From the developer's perspective, they can be categorized in the following main areas:

- Design and Planning (layers, access control, privileges, separation).
- Technology (firewalls, intrusion detection, virus control, encryption).
- Tools (automatic security verification at the design and development level).

Design and Planning involve appropriate selection and application of security architecture. Technology solutions provide implementation details to assure security and trustworthy operation of the system. Currently the authors' work concentrates on the use of tools for safety and security assessment with respect to approved standards [18-19] in the real-time domain.

5. SUMMARY

The paper presents a view on a cohesive approach to treating safety and security issues in industrial control systems. The authors draw from the concept of a safety shell to adopt it to developing security applications. A previously established approach to evaluation of tools in safety-critical systems is also used for assessing security.

6. REFERENCES

[1] Dzung D. et al., Security of Industrial Communication Systems, Proceedings of the IEEE, Vol. 93, No. 6, pp. 1152-1177, June 2005

[2] Stouffer K., J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, MD, Sept. 2008

[3] Koopman P., Embedded System Security, IEEE Computer, pp. 95-97, July 2004

[4] Parameswaran S., T. Wolf, Embedded Systems Security – An Overview, Design Automation for Embedded Systems, Vol. 12, No. 3, pp. 173-183, September 2008

[5] Stammberger K., Current Trends in Cyber Attacks on Mobile and Embedded Systems, Embedded Computing Design, Vol. 7, No. 5, pp. 8-12, September 2009

[6] Wahlström B., IAEA TWG-NPPCI Activities within Computer Security, IAEA Technical Meeting on Cyber Security of Nuclear Power Plant Instrumentation, Control, and Information Systems, Idaho Falls, Idaho USA, October 17–20, 2006

[7] Brooks R.R. et al., Automotive Systems Security: Challenges and State-of-the-Art, Proc. CSIIRW08 Cyber Security and Information Intelligence Research Workshop, Oak Ridge, Tenn., May 12-15, 2008

[8] Halperin D. et al., Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, Proc. SP2008, IEEE Symposium on Security and Privacy, May 18-22, 2008

[9] Shea D.A., Critical Infrastructure: Control Systems and the Terrorist Threat, CRS Report for Congress, Order Code RL31534, Congressional Research Service, Washington, DC, January 20, 2004

[10] Weiss J.M., Testimony of Joseph M. Weiss Control Systems Cyber Security Expert before the Committee on Commerce, Science, and Transportation, U.S. Senate, March 19, 2009, URL: http://commerce.senate.gov/public/_files/WeissTestimony.pdf

[11] Boyes W., Safety, Security and Complex Systems in Critical Infrastructure Protection, Invited Talk, SAFECOMP 2009, 28th International Conference on Computer Safety, Reliability and Security, Hamburg, Germany, September 15-18, 2009. URL: http://www.controlglobal.com/articles/2009/CriticalInfrastructure0909.html

[12] Romanski G., Safe and Secure Partitioned Systems and Their Certification, Proc. WRTP 2009, 30 IFAC Workshop on Real-Time Programming, Mragowo, Poland, October 12-14, 2009, URL: http://www.wrtp-rts.proceedings2009.imcsit.org/pliks/207.pdf

[13] Leveson N., Safeware: System Safety and Computers. Addison-Wesley, Boston, Mass., 1995

[14] Redmill F.J. (Ed.), Dependability of Critical Computer Systems, Vol. I & II. Elsevier Applied Science, London, 1988/89

[15] van Katwijk J., H. Toetenel, A.E.K. Sahraoui, E. Anderson, J. Zalewski, Specification and Verification of a Safety Shell with Statecharts and Extended Timed Graphs. Proc. SAFECOMP 2000, pp. 37-52

[16] Zalewski J., W. Ehrenberger, F. Saglietti, J. Gorski, A. Kornecki, Safety of Computer Control Systems: Challenges and Results in Software Development. Annual Reviews in Control, Vol. 27, No. 1, pp. 23-27, 2003

[17] Gumzej M., M. Colnaric, W. Halang, Safety shell for specification-PEARL oriented UML real-time projects, Computer Languages, Systems and Structures, Vol. 35, No. 3, pp. 277-292, 2009

[18] Kornecki A., J. Zalewski, Experimental Evaluation of Software Development Tools for Safety-Critical Real-Time Systems, Innovations in Systems and Software Engineering - A NASA Journal, Vol. 1, No. 2, pp. 176-188, 2005

[19] Kornecki A., B. Butka, J. Zalewski, Software Tools for Safety-Critical Systems According to DO-254, IEEE Computer, Vol. 41, No. 12, pp. 112-115, December 2008