Chapter 61
Security of Safety Important I&C Systems

Vyacheslav Kharchenko
National Aerospace University- KhAI, Ukraine & Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Andriy Kovalenko
Centre for Safety Infrastructure-Oriented Research and Analysis, Ukraine

Anton Andrashov
Research and Production Corporation Radiy, Ukraine

ABSTRACT

One of the most challenging modern problems–security assessment and assurance for safety important I&C systems–is discussed. Interrelations and hierarchical structure of I&C systems attributes, including safety and security, are considered. Review of existing regulatory documents that covers various development and operation aspects of safety important I&C systems is presented. Such a review also addresses issues related to requirements for safety important I&C systems, including security requirements, depending on their underlying technology, as well as reveals the impact of the main features, including used technologies and development approaches. Main challenging problems and requirements in the area of security assurance for complex safety important I&C systems are outlined. A possible way to analyze the security vulnerabilities of safety important I&C system is considered; it is based on process-product approach, and it requires performance of assessments for products (components of I&C system at different life cycle stages) and all the processes within the product life cycle. A possible approach to assessment and assurance of safety important I&C systems security is discussed. Such an approach takes into account possible vulnerabilities of Field Programmable Gate Arrays (FPGA) technology and appropriate points of their insertion into the life cycle. An analysis of existing techniques for assurance of safety important I&C systems security is performed.

DOI: 10.4018/978-1-4666-8111-8.ch061

INTRODUCTION

I&C systems are complex systems that consist of both hardware and software components, which continuously interact with each other in order to perform their intended functions. One of the development and operation problems of modern I&C systems for critical application is the reliable assessment and assurance of the two main system attributes, namely safety and security. The assessment of security, which also influences the safety of I&C systems and other controlled applications, is a very important, complicated, and challenging problem. During the assessment, it is necessary to take into account a set of various features and factors, their interrelations and interactions. Modern realities require improving I&C systems security, both in terms of requirements and their implementation. Moreover, assurance of security for critical I&C systems is a requirement of national and international regulatory documents, as well as actual practice in safety engineering (IEC 61508, 2010).

The FPGA technology is now being widely used worldwide in process industries and increasingly in I&C systems for various safety and security critical domains, such as Nuclear Power Plants (NPPs), on-board computer-based systems, electronic medical systems, etc. (NUREG/CR-7006, 2010). The application of FPGA technology allows developers to implement the required functions in a convenient and reliable way.

There are several challenging problems in the area of security assurance for complex safety important I&C systems, including the following: consideration of all possible vulnerabilities that can appear in the final product due to process discrepancies, which were presented at earlier stages of the product life cycle, prioritization of such vulnerabilities according to their criticality and severity, determination of both sufficient and cost-effective countermeasures either to eliminate the identified (or potential) vulnerabilities or to make the vulnerabilities difficult to exploit by an adversary. In our opinion, the accurate evaluation of the actual level of the vulnerabilities' criticality and severity (and security of the system in whole) is one of the main challenges. Inaccurate estimation can cause additional efforts, costs and may present undesirable level of risk. In the framework of this chapter, I&C safety is considered as an attribute of high importance. Security is an attribute, which affects safety (Kharchenko, V. et al., 2011).

BACKGROUND

In a modern world, there are many various regulations, which, in general case, cover the most important areas widely used by the mankind. It is possible to distinguish those related (in some way) to safety important I&C systems, grouped into several sets to cover general issues of critical I&C systems at various lifecycle stages (including their development, operation and maintenance), security, as well as covering various technology-related aspects.

But a problem of creating of regulatory base covering simultaneously all the aspects required to develop, use and maintain reliable and secure safety important I&C systems is still challenging. Such regulatory base should also address questions related to processes and products depending on intended use of safety important I&C system, assessment and assurance of certain I&C system attributes, etc.

STATE-OF-ART DOCUMENTS IN THE AREA OF CYBER SECURITY

This subsection provides analysis results for existing documents, both national and international, related to the security of safety important I&C systems.