Development of a New IEC Standard – Requirements for Security Programmes for Computer-Based Systems

Edward L. Quinn
ANS Past President
IEC SC45A WGA9 Convenor
Technology Resources
23292 Pompeii Drive
Dana Point, CA 92629, USA
tedquinn@cox.net
(949) 632-1369

Leroy Hardin
Digital I&C Engineer
U.S. Nuclear Regulatory Commission
RES/DE/DICB
MS: CSB-02A07M
Washington, DC 20555-0001, USA
leroy.hardin@nrc.gov
(301) 251-7929

Ludovic Pietre-Cambacedes
Research-engineer
EDF R&D
1, av. Général de Gaulle
92141 Clamart,
France
ludovic.pietre-cambacedes@edf.fr
+33 1 47 65 43 21

INTRODUCTION

The purpose of this paper is to provide an overview of the development of a new standard by the International Electrotechnical Commission (IEC), focused on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of attacks against computer-based systems.

It is recognized that this is an evolving area of regulatory requirements, due to the changing and evolving nature of the computer security threats. Therefore, the goal of this project is to provide a standard which defines the framework within which the evolving country specific requirements may be developed and applied.

It is also recognized that this subject matter requires protection and limited release of the products derived from application of this standard to country specific requirements to minimize the extent to which organizations, intending to access illegally, improperly or without authorization, a nuclear plant system or systems may benefit from this information.

The increasing use of computers for various functions at nuclear facilities brings forth new vulnerabilities that must be addressed in a rigorous and balanced manner.

Nuclear power plant computers are used in non safety and systems important to safety, where non-availability or malfunction could affect nuclear safety and continuity of power. These computers are also used in the control of access to sensitive areas, where their non-availability or malfunction could permit unauthorized access or deny access to authorized persons. Computers are also used to store important and sensitive data, where any malfunctions could lead to the loss of important data or the unauthorized release of sensitive information. The complexity of these computer systems makes it difficult to identify comprehensively the potential threats to the nuclear facilities.

Experience shows that computer systems without proper protection from attack can become unavailable or unable to fulfill their intended function, and must be protected throughout the whole life cycle.

The proposed standard is intended to be used for operating and new Nuclear Power Plants (NPP). The standard is justified by the necessity to improve the NPP equipment reliability both for operating and new reactors for protection from cyber security attacks.