EAI Endorsed Transactions
on Energy Web and Information Technologies
Research Article EAI.EU

Application of a Hybrid Method for Key Energy Facilities Safety Assessment

I.I. Livshitz [1,*], P.A. Lontsikh [2] and E.P. Kunakov[3]

[1]PhD, SPIIRAS, St. Petersburg, Livshitz.il@yandex.ru
[2]Doctor of Science, Irkutsk National Research Technical University, palon@list.ru
[3]Postgraduate, Irkutsk National Research Technical University, egor-kunakov@mail.ru

Abstract

Information Technologies (hereinafter – the “IT”) without security functions (hereinafter – the “SF”) are the exception rather than the rule nowadays [1 – 4]. Components of IT without SF are not a big problem since they can be replaced by analogs, which SF have, or can be supplemented by the necessary "imposed" SF, or we can "import" the required SF from the adjacent components of IT, which are an integral part of the information processing system (hereinafter – the “IPS”). Speaking further of IT, we will assume that the modern IT components presented in the competitive market for energy facilities (hereinafter – the “EF”) already have a certain set of SF and are able to support IT-security tasks (hereinafter – the “IST”).
Many scientists have done enough research on various safety issues at facilities and published their results [5 – 13]. These studies also concern the causes of various incidents at key facilities, especially energy ones, risk identification, and the analysis of the consequences for safety.
Against this background, the problem of adequate IT-security assessment of the EF is particularly relevant [14 – 16]. Indeed, why should we spend the resources on the implementation of additional "superimposed" SF in IPS, if there is an opportunity to optimize costs by using existing and practically "spent" SF? In this case, a reasonable solution would be to assess the existing level of IT-security related to the architecture of IPS resulting from the composition of IT-components that have SF for key EF [17 – 21]. Based on the results of the evaluation, it is possible to make a decision on the implementation of new additional SF in IPS based on documented facts.

Keywords: Fuel, energy, assessment, security, information, function, risk, vulnerability, threat, ISO, IEC, requirement.

Received on 05 May 2018, accepted on 03 July 2018, published on 28 January 2019

doi: 10.4108/_____

*Corresponding author. Email:Livshitz.il@yandex.ru

1. Problem-solving approaches

The problem in this IT-security subject area can be solved in the presence of the following types of expertize:

(i) Individual expertize (IE) inherent to its carrier. This is the well-known "mega light head". Advantages – compliance with the principle of "it is". Disadvantages – a search for a quality carrier is a non-trivial task, and the aggregation of several carriers is often difficult.
(ii) Template expertize (TE) recorded in the form of documented requirements. These are all well-known normative documents for EF of different levels (for example, IEC 61508, 61511). Advantages – primary sources are available. Disadvantages – a large "division price", hence – a significant error.
(iii) Calculation expertize (CE), based on the composition of measurement and calculation techniques. This is a typical modern approach to engineering and scientific problems. Advantages – accuracy due to