Автоматизация в промышленности 2024. №07
www.avtprom.ru

DOI: 10.25728/avtprom.2024.07.02

И.И. Лившиц (Университет ИТМО)

Исследование влияния «наложенных» мер защиты на оценку уровня полноты функциональной безопасности для объектов критической информационной инфраструктуры

В настоящее время проблема обеспечения безопасности объектов критической информационной инфраструктуры (КИИ) признается актуальной в силу известных инцидентов и компрометации компонентов АСУТП. Экспертное сообщество признает необходимость оценки уровня полноты функциональной безопасности (УПБ) как численной меры, пригодной для формирования безопасности для компонентов АСУТП. Известно несколько подходов для обеспечения безопасности объектов КИИ, среди которых выделим два основных – расчет УПБ для компонентов АСУТП и формирования на основании этих данных численной общей оценки функциональной безопасности (by design) и подход применения «наложенных» (дополнительных) мер защиты, призванных обеспечить требуемый регуляторами уровень безопасности для потенциально уязвимых компонентов АСУТП. В представленной публикации предлагается новая методика, позволяющая оценить безопасность всех объектов КИИ в терминах УПБ – как встроенных функций безопасности, так и «наложенных» мер защиты. В качестве новой методики предлагается выполнять расчет УПБ на основании ГОСТ Р МЭК (IEC) серии 61508 через формирование расчетного значения вероятности опасных отказов по запросу (PFDavg).

Ключевые слова: функциональная безопасность, уровень полноты безопасности, система, объект критической инфраструктуры, аудит, надежность, анализ рисков, остаточный риск, «наложенные» меры защиты.

.

Лившиц Илья Иосифович *– д-р техн. наук, профессор практики, Университет ИТМО.*

Список литературы

1. Костогрызов А.И. Эффективное управление рисками для критически и стратегически важных объектов РФ // ИТ- Стандарт. 2015. № 2(3). С. 1–8.
2. Костогрызов А.И. Пути решения некоторых проблем комплексной безопасности методами системной инженерии // ИТ- Стандарт. 2017. № 4(13). С. 5–12.
3. Латышов К.В., Бондаренко Н.Е., Уксеков В.Д., Малютин М.С. Применение комбинации наложенных и встроенных средств защиты информации на цифровой подстанции // В книге: Радиоэлектроника, электротехника и энергетика. Тр. XXVIII международной научно-технической конференции студентов и аспирантов. Москва, 2022. С. 884.
4. Поляков Г.К. Анализ проблем обоснования рационального состава СЗИ // Тр. XV международной отраслевой научно-технической конференции «Технологии информационного общества». 2021. С. 331-333.
5. Карпенко А.И. Встроенные механизмы информационной безопасности промышленной безопасности и почему ими не стоит пренебрегать // Энергоэксперт. 2019. № 4 (72). С. 78-79.
6. Лившиц И.И., Сунцова Д.И. Численный расчет функциональной безопасности компонентов технически сложных промышленных объектов // Автоматизация в промышленности. 2023. № 7. С. 9-15.
7. Лившиц И.И. Ретроспектива _____проблемы обеспечения безопасности компонентов АСУТП // Автоматизация в промышленности. 2023. № 1. С. 40-46.
8. Ефимов А.О., Лившиц И.И., Мещеряков М.О., Рогозин Е.А., Романова В.Р. Об отдельных аспектах стандартизации и условий функционирования автоматизированных систем // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50. № 4. С. 101-108
9. Лившиц И.И. Исследование оценок защищенности промышленных систем // Автоматизация в промышленности. 2020. № 12. С. 13-18.

Livshits I.I. Investigating the influence of imposed security measures on the estimate of safety integrity level for the objects of critical information infrastructure

Ensuring the security of objects of critical information infrastructure (CII) is still relevant because of the known recent incidents and the compromise of process control components. The expert community acknowledges the need for evaluating the safety integrity level as a quantitative measure suitable for security development of process control components. Several approaches for ensuring CII object security are available, which include two basic ones. The first one presumes SIL calculation for process control components with subsequent development of the quantitative overall functional security (secure by design), the second one is based on imposed (additional) security protection measures aimed at ensuring the mandatory security level for potentially vulnerable components. The paper offers a new procedure enabling the assessment in SIL terms of all CII objects including both embedded security functions and imposed protection measures. It proposes to evaluate SIL on the basis of IEC 61508 through calculating the average probability of failure on demand (PFDavg).

Keywords: *functional safety, safety integrity level, system, object of critical information infrastructure, audit, reliability, risk analysis, residual risk, imposed security protection measures.*