К ВОПРОСУ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ

И.И. Лившиц (Университет ИТМО)

Проблема обеспечения безопасности для промышленных систем управления имеет давнее происхождение, в частности, первые примеры появились еще в XX веке при создании автоматизированных систем управления для объектов атомной, космической и иных отраслей. Важно, что особенностями предыдущих решений было единое архитектурное решение — не существовало раздельного определения сущностей информационных технологий и информационной безопасности. В настоящее время специалисты применяют для решения проблемы обеспечения безопасности международную экспертизу, подробно изложенную в стандартах IEC (ГОСТ Р МЭК) серии 61508 и/или 61511, а также методы обработки рисков в соответствии с требованиями стандартов ISO и ISO/IEC (ГОСТ Р) серии 31000 и/или 27005.

В статье предложено при обеспечении безопасности промышленных систем управления различного назначения учитывать несколько аспектов, в том числе: заданное быстродействие, методы подтверждения соответствия, формирования оценок остаточных рисков и иных исчислимых оценок. Предложено обратить первостепенное внимание на развитие подхода «от функциональности», при котором формирование и решение проблемы начинается в тот момент, когда производитель создает спецификацию на разработку промышленной системы управления, включающую требования функциональной безопасности, и далее проводит оценку по установленным и известным требованиям доверия.

Ключевые слова: безопасность промышленных систем управления, риск, требования функциональной безопасности, требования доверия, киберинцидент.

Введение

Для обеспечения безопасности промышленных АСУ известно несколько подходов, среди которых наибольшее внимание получили: применение «наложенных» средств защиты информации (СЗИ) и тотальная изоляция всех компонентов ИТ-инфраструктуры. Очевидно, что ни один из этих подходов не лишен методических недостатков и не дает гарантий абсолютной стабильности и безопасности промышленных АСУ.

Можно предположить, что наиболее эффективным является известный еще с 40-х годов XX века подход «от функциональности», при котором формирование и решение проблемы обеспечения безопасности промышленных АСУ начинается в момент создания спецификации. Для каждой конкретной промышленной АСУ формируется своя спецификация требований функциональной безопасности, по которой далее проводится оценка по требованиям доверия. Для общего процесса обеспечения безопасности АСУ характерно, что подход «от функциональности» позволяет оперировать численными оценками по известным методикам, утвержденными международными (IEC) и национальными (ГОСТ и ГОСТ Р МЭК) стандартами.

Отметим, что до настоящего времени не сложилась общая практика проектирования и сборки надежной АСУ из компонентов, имеющих доказательства безопасности, проверяемые до необходимого уровня. Предлагается применять подход функциональной безопасности и «собирать» АСУ из компонентов, имеющих доказанный уровень обеспечения безопасности Safety Integrity Level в соответствии с требованиями IEC (ГОСТ Р) серии 61508 и/или 61511 [1, 2].

Требования к обеспечению безопасности промышленных АСУ

Проблема обеспечения безопасности для промышленных АСУ различного назначения (в английской литературе – Industrial Control System, ICS) имеет давнее происхождение. Первые реальные результаты появились еще в XX веке при создании АСУ для сложных технических объектов атомной, космической, морской и иных отраслей. Важно, что особенностями решений той эпохи было единое архитектурное решение — не существовало раздельного определения сущностей информационных технологий (ИТ) и информационной безопасности (ИБ). В связи с этим системы проектировались, создавались, проходили испытания и эксплуатировались как единое целое [2].

В настоящее время специалисты применяют для решения проблемы обеспечения безопасности АСУ международную экспертизу, подробно изложенную в стандартах IEC (ГОСТ Р МЭК) серии 61508

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Уровень полноты безопасности (SIL)	Средняя вероятность опасного отказа при запросе функции безопасности (PFDavg).	Средняя частота опасного отказа в течение часа (PFH)
4	≥ 10^{-5} до < 10^{-4}	≥ 10^{-9} до < 10–8 $ч^{-1}$
3	≥ 10^{-4} до < 10^{-3}	≥ 10^{-8} до < 10^{-7} $ч^{-1}$
2	≥ 10^{-3} до < 10^{-2}	≥ 10^{-7} до < 10^{-6} $ч^{-1}$
1	≥ 10^{-2} до < 10^{-1}	≥ 10^{-6} до < 10^{-5} $ч^{-1}$

Рис. 1. Значения SIL для PFDavg и PFH

и/или 61511 (https://docs.cntd.ru), а также методы обработки рисков в соответствии с требованиями стандартов ISO и ISO/IEC (ГОСТ Р) серии 31000 и/или 27005 (https://www.iso.org/ru). Важным преимуществом методики в системе ISO следует признать установленные ограничения, в частности, по времени, глубине экспертизы, точности результатов и пр. Более подробно требования функциональной безопасности, изложенные в стандартах ISO, рассмотрены в [3 – 5]. Для объективности необходимо отметить систему стандартов NIST, в частности, NIST Special Publication 800-82 Revision 2 «Guide to Industrial Control Systems (ICS) Security» (Руководство по безопасности промышленных систем управления)[1]. Примечательно, что в тексте данного документа содержится множество конкретных рекомендаций для обеспечения ИБ в АСУ, например, постулат, что единственная технология или продукт безопасности не может адекватно защитить ICS (раздел 6, стр. 6-1), проведение процедур аудита (раздел 6, стр. 6-13) или выбор подходящих процедур защиты в соответствии с отраслевым стандартом ISA99 «Industrial Automation and Control Systems Security Standards».

Известно, что минимальные требования функциональной безопасности по IEC 61508-1 - указание информации, которая должна быть документально оформлена для того, чтобы эффективно выполнять все стадии жизненного цикла системы безопасности, в том числе для программного обеспечения (ПО) в (п. 5.1.1). Установлено, что документация должна содержать достаточную информацию, например:

- для управления функциональной безопасностью (п. 5.2);

- для процесса реализации оценки функциональной безопасности, а также результаты, полученные при этой оценке (п. 5.2.3).

Стандарт IEC 61508-1 определяет значения уровня полноты безопасности системы безопасности (Safety Integrity Level, SIL). Показатель SIL имеет целочисленное значение от 1 (минимальный) до 4 (максимальный) и зависит от того, как часто в соответствии с проектным заданием предполагается применение системы безопасности. В простейшем случае SIL1 может быть установлен для автономных некритических производственных систем, отказ которых не предполагает каких-либо существенных последствий, и предполагается запрос функциональной безопасности с низкой частотой. Соответственно, SIL4 требуется для проектирования сложных и ответственных промышленных систем, отказ которых может привести к критическим последствиям, и по этой причине предполагается режим с непрерывной частотой запроса функций безопасности. Частота применения предполагает два значения, в зависимости от вероятности предполагаемого отказа (рис. 1):

- PFH – вероятность опасного отказа в течение часа, рабочий режим с непрерывной частотой запроса («высокий» запрос);

- PFDavg – средняя вероятность опасного отказа при запросе функциональной безопасности («низкий» запрос).

Для практического оценивания возможности «достижения» того или иного конкретного значения SIL применяют метрику SFF (доля безопасных отказов, *Safe Failure Fraction*), которая исчисляет процент неопасных отказов из общего числа отказов. Отметим, что отказ относится к безопасным, если он не представляет опасности для системы (например, включение резервных элементов, предусмотренных документацией). Важным обстоятельством являет факт, что стандарт IEC 61508-1 явно различает два типа компонентов:

- тип A – характеристика отказа определена полностью и отказы установлены;

- тип B – компоненты с неопределенной характеристикой отказа, по крайней мере, одного элемента (например, микропроцессор).

В стандарте IEC 61508-1 определены четыре вида отказов:

- λ_{SU}, безопасные, необнаруживаемые;
- λ_{SD}, безопасные, обнаруживаемые;
- λ_{DD}, опасные, обнаруживаемые;
- λ_{DU}, опасные, необнаруживаемые.

Наибольшее значение для оценивания безопасности АСУ получили последние два типа отказов. Рассмотрим их более подробно:

- λ_{DD} – лямбда обнаруженных опасных отказов (англ. Lambda Dangerous Detected) — число обнаруженных опасных отказов на единицу времени. Показывает число обнаруженных в ходе диагностики опасных отказов на 10^9 часов. Отказ элемента считается опасным, если при его возникновении невозможно выполнить функцию безопасности;

- λDU – лямбда необнаруженных опасных отказов (англ. Lambda Dangerous Undetected) — число необнаруженных опасных отказов на единицу времени, показывает число необнаруженных в ходе диагностики опасных отказов на 10^9 часов.

Отказ считается безопасным, если в случае его возникновения система не переходит в опасное состояние. Соответственно, SFF определяется по формуле:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DU} + \lambda_{DD} + \lambda_S},$$

где $\lambda_s = \lambda_{SU} + \lambda_{SD}$.

SFF и HFT для устройств типа А

SFF (доля безопасных отказов)	HFT (отказоустойчивость оборудования)		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 ... < 90%	SIL 2	SIL 3	SIL 4
90 ... < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Рис. 2. Максимальные уровни полноты безопасности компонентов

SFF и HFT для устройств типа В

SFF (доля безопасных отказов)	HFT (отказоустойчивость оборудования)		
	0	1	2
< 60%	недопустимо	SIL 1	SIL 2
60 ... < 90%	SIL 1	SIL 2	SIL 3
90 ... < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Рис. 3. Максимальные уровни полноты безопасности компонентов

Например, показатель SFF может достигать значения 92%[2].

С учетом различных типов компонентов определение SIL приобретает «многомерность» – важно не только определить значение SIL (что может быть задано директивно), но и определить предел «достижимости» SIL исходя из допуска на отказы аппаратного обеспечения различных типов компонентов (рис. 2 и рис. 3 соответственно). Максимальный уровень SIL, зависящий от допуска на отказы аппаратного обеспечения (тип А) с учетом HFT (англ. *Hardware Fault Tolerance*, отказоустойчивость оборудования) и значение SFF показан на рис. 2.

Максимальный уровень SIL, зависящий от допуска на отказы аппаратного обеспечения (Тип В) с учетом HFT и значение SFF, представлен на рис. 3.

Отметим, что параметр HFT показывает способность аппаратного блока обеспечивать выполнение функции безопасности в случае сбоя или ошибки. Значение отказоустойчивости N означает, что сбои (при N + 1 или выше), могут привести к отказу функции безопасности. Если отказоустойчивость равна нулю (N = 0), то уже первая ошибка может стать причиной отказа функции безопасности. На рис. 3 показан пример недопустимой ситуации для SFF < 60%. Таким образом, различие типов компонентов (тип А или тип В) дает основание критически переосмыслить реалии, при которых невозможно без достаточного оценивания безопасности применять ни «наложенные» СЗИ, ни реализовывать тотальную изоляцию. Строго говоря, такое же требование следует и для архитектур тотальной изоляции, поскольку должна создаваться «равнопрочное» безопасное поле для всей системы.

Оценка соответствия безопасности промышленных систем

Приведенные доводы ставят серьезные научно-практические вызовы перед специалистами, которые настойчиво поддерживают применение «наложенных» СЗИ, поскольку в этом случае не используются никакие методы оценивания SIL, тем более с принятием во внимание типов компонентов. При отсутствии любых методов оценивания (даже субъективных) от производителей СЗИ не представляется возможным гарантировать тот или иной достижимый уровень обеспечения безопасности АСУ. Ситуация может иметь и более критические последствия, поскольку известные «наложенные» СЗИ не проходят оценку соответствия даже в соответствии с законодательством (ФЗ-184, ФЗ-187 - http://www.consultant.ru) по требованиям безопасности в РФ. Возникает противоречие: представители ФСТЭК России неоднократно высказывают позицию регулятора в поддержку только применения «наложенных» СЗИ, например:

- на соответствие требованиям по обеспечению защиты информации в соответствии с руководящими документами ФСТЭК России (например, отсутствия недокументированных возможностей). Известны примеры, когда зарубежные промышленные контроллеры (https://www.securitylab.ru/news/520675.php) содержали «закладки», выявляемые уже после установки на промышленных объектах критической инфраструктуры;
- на соответствие требованиям по обеспечению защиты информации в соответствии с приказом № 31 ФСТЭК России (https://fstec.ru).

В тоже время не уделяется внимание существующим функциям безопасности для ИТ-компонентов промышленных АСУ. Более того, представители ФСТЭК России заявляют, что встроенные функции безопасности (подсистема противоаварийной автоматической защиты, ПАЗ) не учитываются регулятором в качестве меры защиты. Это утверждение было неоднократно озвучено, например, на XXV научно-практической конференции «Комплексная защита информации» (2020 г.)[3] и позже на

[2] https://aumaprivod.ru/docs/files/Functional%20Safety%20%E2%80%93%20SIL.pdf
[3] https://ib-bank.ru/bisjournal/news/14212
[4] https://www.securitylab.ru/blog/personal/valerykomarov/350544.php

конференции ИБ АСУТП[4] (2021 г.). Но при применении «наложенных» СЗИ без должного функционального тестирования этот привнесенный ИТ-компонент становится уже не мерой защиты ИБ, а весьма серьезным риском (особенно при N=0), который резко снижает общую оценку защищенности ПСУ.

Таким образом, исключение из рассмотрения требований функциональной безопасности, а, следовательно, и невыполнение тестирования ИТ-компонента целиком (не по отдельности на соответствие требованиям функциональной безопасности и Приказа ФСТЭК) не приводит к доказанному повышению уровня полноты безопасности, а, напротив, снижает существующий «запас прочности». Обратимся к системе международных, национальных и отраслевых стандартов, посвященных обеспечению функциональной безопасности на объектах критической инфраструктуры. Помимо уже известного стандарта IEC (ГОСТ Р МЭК) серии 61508 и 61511 применяются IEC (ГОСТ Р МЭК) серии 62425 для систем железнодорожной автоматики (безопасность электронных систем сигнализации) и IEC (ГОСТ Р МЭК) серии 61513 (https://docs.cntd.ru/document/1200089290) для систем контроля и управления атомными станциями соответственно. Разработаны также Технические регламенты Таможенного Союза (ТР ТС):

- ТР ТС 001/2011 «О безопасности железнодорожного подвижного состава»;
- ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта»;
- ТР ТС 002/2011 «О безопасности высокоскоростного железнодорожного подвижного состава».

Иерархия управления в АСУ

С учетом иерархии управления в АСУ очевидно, что для каждого уровня должны быть явно определены свои требования, и чем ниже уровень управления, тем более жесткие должны быть требования к обеспечению функциональной безопасности. Соответственно, вопрос применения «наложенных» СЗИ, способных обеспечить информационный обмен (прием информации с датчиков, анализ и выдачу управляющего воздействия) с гарантированным откликом в установленное нормативное время (секунды и менее для уровня промышленных контроллеров, ПЛК) вызывает серьезные сомнения, поскольку является областью неопределенности и значимого риска. Дополнительно учтем требования IEC (ГОСТ Р МЭК) серии 61508 и/или 61511, согласно которым все пространства состояний (возможные сочетания открытых клапанов, вентилей, положений манипуляторов и пр.), а также переходы между ними должны быть заранее определены и многократно протестированы на уровне всех ИТ-компонентов в АСУ. В обязательном случае реализуется контур безопасности (ПАЗ), который, уместно напомнить, является обязательной и неотъемлемой частью любой АСУ.

Вызывает серьезное сомнение способность «наложенных» СЗИ «выдать» в канал управления верное управляющее воздействие, согласующееся с реакцией встроенной ПАЗ (следует принять во внимание, что это быстродействие на самом нижнем, «полевом» уровне, должно составлять 10^{-3} – 10^{-6} с.). В наилучшем случае «наложенное» СЗИ успевает сработать не позднее ПАЗ, но возникает не менее важная следующая проблема – арбитраж между «логикой» управления ПАЗ (зачастую является коммерческой тайной каждого производителя) и «логикой» СЗИ, также не являющейся публично доступной.

В качестве хорошего практического примера приведем актуальное руководство «PLC Security Top 20 List»[5], которое содержит 20 рекомендаций по конфигурированию устойчивого ПЛК на случай наличия некорректных настроек сети или киберинцидентов. Отмечается, что ПЛК, конечно, не является СЗИ и не должно обеспечивать защиту от киберинцидентов, тем не менее, в силу заложенных правильных механизмов функциональной безопасности они могут минимизировать ущерб от киберинцидентов для физических процессов. Данное руководство включает требования, посвященные контролю целостности (логики ПЛК, таймеров и счетчиков, значений ввода/вывода), устойчивости и мониторингу определенных значений в ПЛК, которые могут указывать на проблемы безопасности. В руководстве даны прямые ссылки на хорошие практики в области ИБ (в частности, ISO/IEC 27001), но отмечаются требования, не разделяемые между «чистым» ИТ и «чистой» ИБ, например: разделение кода ПЛК на модули для упрощения тестирования; постоянно активированный режим с оповещением об отключении; использование контрольных сумм для проверки на наличие проблем целостности кода; отключение ненужных портов и протоколов и пр. Этот пример показывает, насколько важно обеспечить единый, сбалансированный подход «от функциональности», не сваливаясь в единственные альтернативы «наложенных» СЗИ или тотальной изоляции. Все, что необходимо для обеспечения функциональности, уже заложено при проектировании в доверенные ИТ-компоненты для создания безопасных АСУ.

Заключение

1. Формирование и решение поставленной проблемы по обеспечению безопасности промышленных систем управления различного назначения актуально и требует комплексного учета многих факторов: устаревшего подхода моделей

[5] https://gca.isa.org/blog/the-top-20-secure-plc-coding-practices-project

угроз, игнорирования IEC (ГОСТ Р МЭК) и иных актуальных риск-ориентированных стандартов, попыток раздельного анализа ИТ-компонентов и «наложенных» СЗИ.

2. Необходимо проблему обеспечения безопасности промышленных систем управления рассматривать в аспектах: заданного быстродействия, методов подтверждения соответствия, формирования оценок остаточных рисков и иных исчислимых оценок.

3. Требуется уделять первостепенное внимание развитию подхода «от функциональности», при котором формирование и решение проблемы начинается в тот момент, когда производитель создает спецификацию на разработку промышленной системы управления, включающую требования функциональной безопасности, и далее проводит оценку по установленным и известным требованиям доверия.

4. Для решения проблемы обеспечения безопасности промышленных систем больше внимания следует уделять поставке ИТ-компонентов, безопасных изначально и прошедших объективную оценку соответствия функций безопасности в аккредитованных лабораториях в соответствии с требованиями применимых международных и национальных стандартов.

Список литературы

1. *Лившиц И.И.* Аудит информационной безопасности объектов топливно-энергетического комплекса // Энергобезопасность и энергосбережение. 2021. № 1. С. 5-12.
2. *Лившиц И.И.* К вопросу обеспечения безопасности промышленных систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 1. С. 1-14.
3. *Livshitz I.I., Neklyudov A.V., Lontsikh P.A.* IT security evaluation — "hybryd" approach and risk of its implementation // Journal of Physics: Conference Series. 2018. V. 1015. N 4. P. 042030.
4. *Лившиц И.И.* Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов // Труды СПИИРАН. 2020. Т. 19. № 2. С. 383–411.
5. *Лившиц И.И.* Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности. 2020. № 1(35). С. 42–51.

Лившиц Илья Иосифович *– д-р техн. наук, проф. практики, Университет ИТМО.*
E-mail: livshitz.il@yandex.ru