Комплексная безопасность систем реального времени

Сергей ЗЫЛЬ,
к. т. н., генеральный директор ООО «НИЦ ФБ»

Системы реального времени

Для обсуждения такой масштабной темы, как комплексная безопасность систем реального времени, необходимо пояснить, что мы имеем в виду под понятием «система реального времени» и в чем заключается комплексность ее безопасности.

Система реального времени отличается от информационной системы тем, что последняя предназначена для ввода, хранения, преобразования и выдачи информации, а система реального времени – для управления физическими объектами. Другими словами, защищаемым активом в информационной системе является информация, а в системе реального времени – оборудование.

В качестве иллюстрации приведем модель уровней защиты в перерабатывающей промышленности (рис. 1).

На рис. 1 представлен управляемый объект (УО). В качестве такового с равным успехом можно было бы указать управляемый процесс. Казалось бы, управляемый объект – это и есть тот актив, который нужно защитить. Но нет, есть объекты защиты поважнее – люди и окружающая среда. Причем люди – это не только эксплуатирующий персонал управляемого объекта, но и его охрана, а также жители близлежащих населенных пунктов и даже грибники, которые забрели близко к управляемому объекту.

Пусть для мониторинга и диспетчерского контроля управляемого объекта используется АСУ ТП, например, на основе SCADA-системы. АСУ ТП потому «автоматизированная», а не «автоматическая», что в контуре управления есть человек-оператор. Со всеми своими сильными и слабыми сторонами.

Эксплуатирующий персонал может допускать ошибки, в АСУ ТП могут происходить отказы. Из-за этого в УО могут возникать проблемы или УО сама может стать проблемой. Поэтому нужно то, что обычно называют противоаварийной защитой (ПАЗ).

То, чем занимается ПАЗ, называют функциональной безопасностью. ПАЗ – это автоматическая система. То есть в контуре безопасности не должно быть человека, в отличие от контура управления. Как вы догадались, это необходимо для минимизации человеческого фактора (справедливости ради стоит отметить, он все равно остается, так как, например, монтаж и обслуживание никто не отменял).

Теперь у нас есть все (почти) элементы, чтобы наконец-то приступить к обсуждению комплексной безопасности систем реального времени.

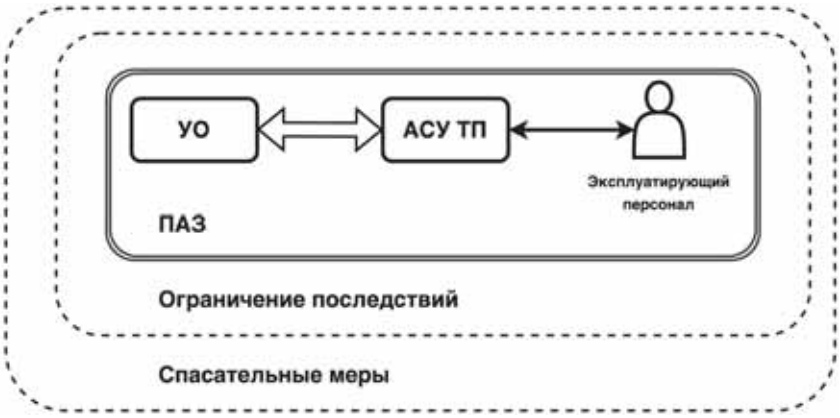

Рис. 1. *Модель уровней защиты в перерабатывающей промышленности*

Рис. 2. *Иерархия задач информационной безопасности*

Что же случится, если оператор не справится с управлением АСУ ТП, и при этом в ПАЗ произойдет отказ? Может произойти (а может и не произойти) авария. Поэтому дополнительно нужно предусматривать меры ограничения последствий и, не про нас будет сказано, спасательные меры.

Средства ограничения последствий – это, например, ограждения и рвы, препятствующие распространению вредной субстанции. Помните слово firewall? Оно, вообще-то, отсюда, из области ограничения последствий. К ним также относятся системы пожаротушения и аварийной сигнализации, поскольку они срабатывают уже по факту инцидента.

Здесь, кстати, можно заметить еще одну характерную черту систем управления и особенно систем противоаварийной защиты – они должны предотвращать аварии. В терминах управления рисками – они должны обеспечивать снижения риска. И вот мы незаметно оказались в зоне ответственности информационной безопасности – управлении рисками активов.

Итак, давайте уточним понятие «система реального времени». Под этим понятием будем иметь в виду:

- автоматизированные системы управления технологическими процессами (АСУ ТП);
- контроллеры и звенья систем автоматики, например, контрольно-измерительные приборы (КИП) и программируемые логические контроллеры (ПЛК);
- системы телеметрии, телемеханики и дистанционного управления;
- приборные системы безопасности (ПСБ), в частности, системы противоаварийной защиты.

Распространенный синоним для систем реального времени – киберфизическая система (Cyber-Physical System).

Кибербезопасность, функциональная безопасность и надежность – что важнее?

Исходя из сказанного, часто возникает вопрос: а есть ли вообще проблема информационной безопасности применительно к системам реального времени? Отвечу – очень даже есть. Главный риск информационной безопасности для промышленной системы – это манипуляция объектом управления.

Конечно, все мы знаем, что хранение конфиденциального документа в несгораемом сейфе – тоже информационная безопасность. Поэтому более корректно использовать термин «кибербезопасность», который вводится в стандартах серии МЭК 62443. Этот же стандарт подчеркивает приоритеты обеспечения конфиденциальности, целостности и доступности для информационных систем и систем реального времени (рис. 2).

Итак, безопасность системы реального времени – это не столько конфиденциальность и совсем не только про компьютеры. Это комплексное понятие, которое включает два неразрывно связанных друг с другом и взаимодополняющих аспекта – функциональную безопасность и кибербезопасность, которая понимается как специализированная версия информационной безопасности.

Рис. 3. *Функциональная безопасность vs надежность*

Функциональная безопасность – способность системы функционировать, не создавая неприемлемого риска для жизни или здоровья людей, состояния окружающей среды либо сохранности материальных ценностей. Функциональная безопасность – ключевая характеристика системы реального времени в ряде областей применения, например, в атомной энергетике или медицине.

Кибербезопасность – это меры по предотвращению умышленного или неумышленного вмешательства в штатную и запланированную работу системы реального времени. Выделение кибербезопасности как отдельного понятия может восприниматься разработчиками систем реального времени как искусственное, однако оно позволяет правильно расставить акценты, учитывающие особенности решаемых задач.

Принцип комплексной безопасности системы реального времени может быть сформулирован следующим образом: система реального времени не является функционально безопасной, если не обеспечена кибербезопасность, система реального времени не является информационно безопасной, если не обеспечена функциональная безопасность. Это как две стороны одной медали.

Вы можете спросить: может быть, функциональная безопасность – это хорошо всем известная надежность? И да, и нет. Проиллюстрируем это с помощью рис. 3.

На рис. 3 схематично, не в масштабе, показано, что понятия функциональной безопасности и надежности отнюдь не тождественны. Чтобы не терять из виду «комплексность» проблематики безопасности систем реального времени, мы добавили в схему элемент «кибербезопасность».

> Функциональная безопасность – ключевая характеристика системы реального времени в ряде областей применения.

Рис. 4. *Распределение опасных дефектов по этапам жизненного цикла*

Надежность – количественная характеристика. Например, для ее измерения часто используют коэффициент готовности – выраженное в процентах отношение среднего времени наработки на отказ к среднему времени восстановления. Если УО – это медицинское оборудование вентиляции легких, то функциональная безопасность, действительно, достигается повышением надежности. В системах же аварийного отключения, напротив, обеспечение функциональной безопасности достигается мерами, снижающими время наработки на отказ УО, т. е. уменьшающими коэффициент готовности.

Ситуация с надежностью осложняется тем, что методы ее расчета – статистические и применимы к «случайным отказам» (random faults) технических средств. Проблема в том, что такие отказы становятся причиной примерно 10% инцидентов в промышленности. «Оставшиеся» 90% относятся к системным отказам (systematic faults), которые закладываются на разных этапах жизненного цикла системы реального времени (рис. 4).

Из рис. 4 видно, что отнюдь не разработчики вносят основной вклад в отказы систем. Кроме того, к особенностям систем реального времени, в отличие от информационных систем общего назначения, относятся сложность и даже невозможность устранения дефектов, в том числе уязвимостей, на этапе эксплуатации. Например, медицинское оборудование прошло клинические испытания и поставлено в сотни медицинских учреждений, после чего найдена уязвимость – устранить уязвимость методом рассылки патчей в IT-службы медучреждений для самостоятельной установки и настройки не представляется возможным, более того, создается дополнительный риск фатальных отказов неприемлемого уровня.

Вся надежда на предотвращение отказов и эффективное управление ими в процессе эксплуатации. Но как же оценить

Рис. 5. *Модель управления рисками МЭК 61508*

наличие или отсутствие в проекте системных ошибок? И вот здесь нам не обойтись без ГОСТ Р МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». Это базовый стандарт в области функциональной безопасности. Что значит «базовый»? Дело в том, что отраслей промышленности и вообще человеческой деятельности, в которых необходимо управлять рисками функциональной безопасности, достаточно много, и каждая из них уникальна. Например, в химической промышленности, на автомобильном и железнодорожном транспорте риски применения вычислительной техники существенно различаются, и меры снижения рисков тоже отличаются.

МЭК 61508 – межотраслевая методология функциональной безопасности

Международная электротехническая комиссия разработала единую фундаментальную межотраслевую методологию, которая содержится именно в МЭК 61508. Вот что включает данная методология:

- модель управления рисками (рис. 5);
- V-модель разработки (рис. 6);
- уровни полноты безопасности (SIL);
- категорирование отказов на системные, случайные и отказы по общей причине;
- перечень методов и средств для предотвращения и снижения последствий системных отказов аппаратного и программного обеспечения, отказов аппаратного обеспечения по общей причине, которые должны быть реализованы на каждом из этапов V-модели для достижения заданного уровня SIL.

Представленная на рис. 5 упрощенная модель управления рисками функциональной безопасности включает понятия риска, создаваемого системой реального времени, допустимого риска, необходимого снижения риска, фактического снижения риска и остаточного риска. Это важно понимать – нет и не может быть 100%-ных гарантий безопасности, всегда есть остаточный риск.

V-модели жизненных циклов разработки технических средств и программного обеспечения,

Рис. 6. *Каноническая V-модель разработки*

конечно, несколько отличаются. На рис. 6 представлен «программный» вариант. Конечно, не нужно, чтобы жизненный цикл разработки был именно такой, как показывает стандарт, – модель на то и модель, чтобы служить ориентиром, а не безусловным правилом. Суть заключается в выполнении при разработке всех необходимых действий.

Четыре уровня полноты безопасности (сокращенно УПБ или SIL, от англ. Safety Integrity Level) задаются на основе диапазонов вероятностей отказов. Условно их смысл следующий:

SIL4 – при отказе системы безопасности возможна массовая гибель людей. Речь может идти о поезде или самолете;

SIL3 – при отказе системы безопасности возможна гибель одного или нескольких людей. Это может быть лифт;

SIL2 – возможно тяжелое увечье человека. Например, при работе на станке с движущимися деталями;

SIL1 – угрозы для людей нет, но может быть повреждено дорогостоящее оборудование.

МЭК 61508 учитывает также разницу в характере применения систем реального времени в различных отраслях. В частности, система реального времени может быть:

– системой, срабатывающей по редким, реже одного раза в год, запросам (характерно для нефтеперерабатывающей промышленности – серия стандартов МЭК 61511);
– системой с частым срабатыванием (характерно для автомобильного транспорта – серия стандартов ИСО 26262);
– системой непрерывного использования (характерно для медицины – серия стандартов МЭК 60601).

МЭК 62443 – кибербезопасность промышленных систем

Боюсь, за всеми деталями функциональной безопасности потерялась кибербезопасность. Поэтому есть смысл напомнить о стандартах серии IEC 62443 и объяснить, почему они важны.

> Основное отличие систем реального времени от информационных заключается непосредственно в защищаемом активе.

Серия стандартов IEC 62443 включает 12 частей, разделенных на четыре уровня. Три части переведены на русский язык и приняты в качестве ГОСТов. Непосредственно к уровню вычислительных устройств относятся обе части четвертого уровня (IEC 62442-4-1 и IEC 62443-4-2), на русский язык не переведенные. Первая из них устанавливает требования к безопасной разработке аналогично ГОСТ Р 56939-2016, вторая – технические требования кибербезопасности аналогично профилям защиты, разработанным ФСТЭК России.

Серия стандартов IEC 62443 обеспечивает адаптацию методологии серии стандартов ИСО/МЭК 27000 для промышленной автоматизации. При этом, например, особенностью стандарта IEC 62442-4-1 является то обстоятельство, что он гармонизирован с V-моделью жизненного цикла, представленной в ГОСТ Р МЭК 61508. Из этого вытекает совместимость с отраслевыми стандартами в области функциональной безопасности, основанными на методологии МЭК 61508.

Таким образом, комплексная безопасность систем реального времени основана на рискориентированном подходе и включает сложный комплекс организационно-технических мероприятий, который можно разделить на следующие составные части:

– инвентаризация, анализ и оценка угроз и рисков, среди результатов которых определяются требования к системе реального времени и, как следствие, к ее вычислительным средствам и программному обеспечению, уровням полноты функциональной безопасности (SIL), стойкости к систематическим отказам (ССО) и уровням и классам информационной безопасности;
– требования уровней безопасности с помощью стандартов и нормативных документов транслируются в значительное количество мер, методов и средств, которые должны быть запланированы, выполнены (применены) и проверены на всех этапах жизненного цикла, который, в свою очередь, должен соответствовать V-модели.

Таким образом, с точки зрения безопасности основное отличие систем реального времени от информационных заключается непосредственно в защищаемом активе: актив системы реального времени – это не информация, а управляемый физический объект.

Конечно, мы коснулись только верхушки айсберга. Главные ноу-хау ведущих мировых производителей, на наш взгляд, содержатся непосредственно в методах и средствах, одно перечисление которых с краткими описаниями составляет десятки страниц. Их освоение, внедрение в процессы разработки, создание инструментальных средств их поддержки и методик их применения – вот направления технологического развития предприятий-разработчиков систем реального времени. ■