DOI: 10.22184/1992-4178.2022.219.8.104.108

Углубление самоконтроля контрольно-проверочной аппаратуры изделий систем управления: уточнения и дополнения к предыдущим материалам

С. Белов[1]

УДК 621.317.799 + 53.089.6 + 53.087.4 + 004.42 | ВАК 2.2.8

Углубление самоконтроля контрольно-проверочной аппаратуры (далее – КПА) изделий систем управления (далее – ИСУ). Уточняется и дополняется информация по написанным ранее материалам:

- однократные и многократные тесты плат расширения и жгутов [1];
- расширение областей контроля (системные комплектующие, соответствие плат расширения их руководствам по эксплуатации) [2];
- самоконтроль плат аналогового ввода до сборки аппаратуры [3].

Добавляются новые механизмы углубления самоконтроля (например, поиск изломов в жгутах).

ВВЕДЕНИЕ

Методы, описанные в перечисленных выше материалах, применялись в течение длительного периода времени. Это привело к возникновению ситуаций, требующих уточнений. Эти ситуации, в свою очередь, привели к разработке новых методов самоконтроля КПА, в том числе касающихся ее защиты от несанкционированного доступа, правильного выбора операционной системы, контроля целостности жгутов.

ИДЕНТИФИКАЦИЯ ПЛАТ С РАЗЪЕМАМИ ISA

При самоконтроле КПА его выходные жгуты подключены к встроенным в КПА отдельным разъемам самоконтроля или к специальному жгуту самоконтроля. Самоконтроль проводится с периодичностью один раз в три года, с использованием отдельного ПО.

После успешного самоконтроля и соответствующей отметки ОТК, КПА допускается для работ с ИСУ. Жгуты КПА подключаются к ИСУ. Однако операции с ИСУ недопустимы до проведения облегченного самоконтроля КПА непосредственно перед работой с ИСУ (например, нужно определить повреждение жгутов при подключении к ИСУ). Такой самоконтроль реализуется в считывающем телеметрию ПО как первый тест, разблокирующий остальные тесты. Облегченность диктуется, в числе других причин, изменением распределения сигналов на выходных разъемах жгутов КПА, исключающим подачу сигналов с выходов КПА на ее собственные входы. Возникает патовая ситуация: требуется проверка работы конкретной платы, но работать с ней при этом еще нельзя.

В результате становится возможным проверить у плат только наличие их в системе, открытие, закрытие, выход на режим, присвоение идентификатора, считывание каких-то отдельных безопасных сигналов.

Проблема осложняется тем, что в КПА (как в высокоскоростной промышленной ЭВМ) используются платы с разъемами ISA, управляемые через прерывания. Так как данные платы не имеют драйвера – проверка их работоспособности средствами Windows невозможна.

Однако в инструкции производителя указывается количество байт, занимаемых платой в памяти системы. Из них определенное количество байт плата занимает постоянно (выявляется эмпирически). Последние оставшиеся байты могут занимать таймеры и иные ресурсы платы.

Используя данную особенность, можно сканировать адреса памяти и выявлять комбинации байтов (а также их содержимое), соответствующие конкретным платам ISA. Между платами всегда присутствуют разрывы в виде «пустых» адресов с ненулевыми значениями 65535 или –1.

[1] АО «ГосНИИП», ведущий инженер, for-work2016@mail.ru.

На практическом примере Advantech PCL-730 с условным адресом 0x250, заранее прописанным в Т3, и занимаемым объемом 4 адреса [4]:

- эмпирически определяется количество адресов, всегда занимаемых платой (3 из 4 – недостающий адрес драйвер платы решает занимать не сразу);
- если по адресам 0x250–0x252 считаны числа 65535 – плата отсутствует полностью. Если числа 65535 считываются частично – адрес платы смещен;
- если по адресам 0x250–0x252 считаны числа не 65535, а по граничным адресам 0x249 и 0x254 считаны числа 65535 – плата присутствует с правильным адресом;
- итого по плате PCL-730: стабильно заняты 3 адреса, последний адрес по результатам тестов никогда не отличался от 65535, пустота по границам платы 0x249 и 0x254 постоянна.

На практическом примере Advantech PCL-720 с условным адресом 0x270, заранее прописанным в Т3, и занимаемым объемом 4 адреса [5]:

- эмпирически определяется количество адресов, всегда занимаемых платой (5 из 4 – лишний адрес занимает постоянно какой-то ресурс платы);
- если по адресам 0x270–0x274 считаны числа 65535 – плата отсутствует. Если числа 65535 считываются частично – адрес платы смещен на несколько позиций;
- если по адресам 0x270–0x274 считаны числа не 65535, а по граничным адресам 0x269 и 0x278 считаны числа 65535 – плата присутствует с правильным адресом;
- итого по плате PCL-720: стабильно заняты 5 адресов, адрес 0x275 – изменчив, последний адрес по результатам тестов никогда не отличался от 65535, пустота по границам платы 0x269 и 0x278 постоянна.

Стоит уточнить, что в ОС младше Windows 2000 работа с прерываниями заблокирована самой ОС. В этом случае нужно использовать сторонние библиотеки вида inpout32.dll (конкретно эта – проверена на Windows 7 и Windows XP [6]). Если не использовать библиотеки – функция чтения данных с порта будет всегда возвращать число 0.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИИ BIOS В АДРЕСАХ МИКРОСХЕМЫ WINBOND В СОСТАВЕ МАТЕРИНСКОЙ ПЛАТЫ

При сканировании портов выяснилось, что первые примерно 0x70 адресов (в зависимости от материнской платы) занимает BIOS. Данный диапазон адресов может быть интересен контролем параметров системы. Например, 0x47 – типичное расположение скорости вращения вентилятора процессора (проверено на микросхемах Winbond 83627DHG и 83627(H)F-G).

КОНТРОЛЬ АКТИВНОСТИ СЕТЕВЫХ ПОДКЛЮЧЕНИЙ

Активное сетевое подключение приводит к искажению показаний телеметрии из-за их смещения во времени (имитация ОС Windows жесткого реального времени перестает быть таковой). Проверено получением телеметрии с определенного ИСУ при разном поведении локальной вычислительной сети (далее – ЛВС).

ЛВС может работать в разных режимах: прием-передача мелких пакетов (до 255 байт), прием-передача крупных пакетов (предположительно, до 65 500 байт), сетевое подключение активно без передачи пакетов, сетевое подключение неактивно (вынут сетевой кабель), сетевое подключение отключено (сетевая карта отключена в диспетчере устройств). Смещения во времени носят вероятностный характер при активном подключении – появляется вероятность ложных результатов при диагностике ИСУ. Полученное на практике запаздывание на 1 мс (прием-передача мелких пакетов) может быть критичным при цикле снятия телеметрии 2 мс.

При проверке состояния сетевых подключений API-функцией InternetGetConnectedState следует учитывать ее зависимость от службы SENS (уведомление о системных событиях). Служба SENS, в свою очередь, зависит от службы EventSystem (система событий COM+). Иначе возникает ложноположительный результат: состояние подключения «18» (0x12 – не необходимое 0x10 или 0x20), функция возвращает true вместо false.

Параметр dwReserved всегда должен быть равен 0, независимо от количества сетевых карт в системе и количества активных подключений.

Функция срабатывает мгновенно только при старте системы – в дальнейшем требуется задержка 1 мин после любого изменения состояния сетевого подключения из приведенного выше перечня возможных режимов работы ЛВС [7].

Для контроля статуса службы («запущена») необходимо выполнить команду «sc query имя_службы | findstr RUNNING». Если служба запущена – возвращается строка «STATE: 4 RUNNING», если не запущена – пустая строка. Для сохранения данного результата в текстовый файл: использовать программу TEE, добавляя команду: «| „Полный_путь_tee.exe“ „Полный_путь_лога“ /f». Для работы без программы TEE (получение данных в переменную ПО) нужно использовать функции CreateProcess и CreatePipe.

ЗАЩИТА ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ (ПРОИЗВОДСТВА) КПА И ПО В ЕГО СОСТАВЕ

С целью защиты КПА от незаконного копирования, можно защитить ПО в ее составе, внедрив защищенный ключ с информацией о комплектующих [8, 9]. Выпущенная в 2014 году программа «Защитник ПО» [10]

подходит для данной задачи. На момент ее написания учитывалась кроссплатформенность в рамках семейства ОС Windows, поэтому программа остается полнофункциональной и на Windows 10:

- привязка ПО к нестандартным компонентам КПА (например, к серийному номеру батареи ноутбука или версии BIOS в составе материнской платы);
- обеспечение жесткой и/или мягкой привязки к комплектующим. Например, серийный номер и/или марка/модель комплектующего изделия;
- создание из любой флеш-памяти, независимо от записанного на ней содержимого, аналога ключа eToken. Запуск ПО без данной флеш-памяти будет невозможен;
- редактирование существующих ключей (например, при изменении конфигурации КПА во время выполнения ремонтных работ).

Таким образом, при запуске ПО самоконтроля оно будет проводить самоконтроль самого себя и решать, прерывать ли собственный запуск. Ту же концепцию можно применять и к программе контроля ИСУ в составе КПА.

ВЫБОР ОПТИМАЛЬНОГО ДИСТРИБУТИВА ОС ПО КРИТЕРИЯМ СКОРОСТИ РАБОТЫ ПО КПА И ОТСУТСТВИЯ ВРЕМЕННЫХ ЗАДЕРЖЕК ПРИ ЕГО РАБОТЕ

В интернете существует множество любительских сборок различных поколений ОС Windows. Несмотря на то, что сборки составляются, в основном, для бытовых/игровых/файловых целей, удалось найти дистрибутив, свойства которого применимы к КПА. Выбор поколения Windows XP вызван тем, что, начиная с Windows Vista, работа с портами напрямую затруднена: на практике сама ОС блокирует попытки чтения/записи. Добавляется проблема наличия драйверов для плат расширения.

Windows XP 75MB Edition – пользовательская сборка, главной целью которой был запуск игры Quake 2 с высоким FPS. Конечный вариант сборки оказался настолько качественно и сильно урезанным, что Windows способна функционировать корректно с запущенной всего лишь одной службой RpcSS (удаленный вызов процедур (RPC)).

Урезанность Windows XP привела к неожиданным и критически важным свойствам дистрибутива [11], полезным для КПА. Эти свойства недоступны в обычных дистрибутивах и любительских сборках малого размера, вида Tablet PC Edition, Atom, Small and Fast:

- ПО, запущенное в графическом режиме, показало увеличение частоты с 52,5 Гц в обычной Windows XP до 55 Гц в тестируемой ОС (скорость обновления интерфейса выше на 5,8%). То же ПО, запущенное в фоновом режиме, показало увеличение частоты с 834 до 1082 Гц (скорость обработки исходного кода выше на 29,7%). Для тестирования использовалось ПО получения телеметрии с большим количеством элементов интерфейса [12];
- приоритет реального времени для файлов выставляется настоящий (даже курсор не реагирует на движения мыши). В обычной Windows XP это недостижимо: ОС всегда опускает приоритет приложения до высокого;
- количество служб (в том числе включенных по умолчанию) – минимально.

Данный дистрибутив является наиболее приближенным к ОС жесткого реального времени из поколения Windows XP. 13-летняя поддержка поколения уже окончена [13], но оно продолжает показывать преимущества перед другими ОС. Windows XP 75MB Edition может быть стабильнее Windows 2000, как ОС жесткого реального времени, с учетом потребляемых ресурсов системы и меньшего количества запущенных приложений/библиотек в фоновом режиме.

ИСПОЛЬЗОВАНИЕ СОБСТВЕННЫХ ДИАГНОСТИЧЕСКИХ ПЕЧАТНЫХ ПЛАТ ДЛЯ РАСШИРЕНИЯ ФУНКЦИОНАЛА САМОКОНТРОЛЯ

Приведем пример командного взаимодействия сотрудника-электроника с сотрудником-программистом при разработке КПА с нуля под новое изделие и с новыми требованиями заказчика.

При проведении самоконтроля было обнаружено чрезмерное падение сигнала на одном из каналов платы аналогового ввода. При разборке электрического соединения был последовательно измерен сигнал на разных участках цепи. Поверенный высокоточный мультиметр показывал корректное значение – предполагается ошибка программиста. Однако анализ исходного кода и платы аналогового ввода (с помощью сторонних сигналов) демонстрировал и их полную исправность – предполагается ошибка электроника.

Дилемму решило создание проходника между платой аналогового ввода и жгутом [14]. Выяснилось, что сигнал, действительно, чрезмерно падает при достижении определенного номинала тока в одной из частей блока сопряжения. В итоге обнаружился резистор, забирающий часть сигнала на себя именно в момент проведения теста. Значит, чрезмерное падение сигнала есть норма – и в ПО самоконтроля под этот сигнал были исправлены пределы допустимого значения.

Также была разработана диагностическая печатная плата для экспресс-тестирования блока питания в составе блока системного [15].

ОТСЛЕЖИВАНИЕ ЕДИНИЧНЫХ ПРОМЕЖУТОЧНЫХ И НУЛЕВЫХ ЗНАЧЕНИЙ НАПРЯЖЕНИЙ ОТНОСИТЕЛЬНО НОМИНАЛЬНОГО – ДЛЯ ВЫЯВЛЕНИЯ ИЗЛОМА ПРОВОДНИКА

Излом (разрыв) проводника в сочетании с неразорванной изоляцией провода порождает ситуацию, именуемую далее «недоразрыв». Изоляция провода за счет собственной упругости препятствует полному размыканию проводника. В зависимости от различных по номиналу механических напряжений и эластичности изоляции, возможны варианты:

- проводник соединяется по всей площади. Влияния на КПА нет до нарушения состояния покоя проводника;
- проводник не соединяется. Влияние на КПА выражается в результате теста самоконтроля «не норма»;
- проводник соединяется не по всей площади. Внешний фактор: упругость изоляции. Сопротивление проводника в данном месте повышается. Часть напряжения от нагрузки переходит в место недоразрыва. С учетом того, что изоляция прижимает проводник именно в этом состоянии, – на КПА будет регистрироваться пониженное напряжение, независимо от усреднения результатов, полученных с плат аналогового ввода. При этом оно может входить в допуск при проведении самоконтроля;
- проводник то соединяется, то не соединяется. Внешние факторы: вибрации, однократные воздействия (в том числе потоком воздуха).

Состав тестового стенда, созданного для макетирования двух последних ситуаций:

- плата аналогового ввода Advantech PCI-1713U;
- стандартная ЭВМ с ТТХ, перекрывающими системные требования платы аналогового ввода;
- источник питания Gwinstek SPS-3610 с напряжением 9,7 В;
- мультиметр Appa 205;
- провод диаметром 2,6 мм, заявленным сечением проводника 0,75 мм^2;
- два параллельных резистора SQP 20 Ом / 15Вт / ±5%;
- штыри из разъема DB37 для надежного контактирования с каналами платы аналогового ввода;
- ПО снятия данных с платы аналогового ввода [12]. Частота съема данных в фоновом режиме 1081 Гц, в реальном времени – 55 Гц;
- снятые данные с платы не усредняются и не округляются.

Тестируемый провод изгибался из прямого состояния в полностью сложенное, складывался с приложением значительного усилия, что гарантированно создавало единственно возможное место излома. После получения на мультиметре подтверждения желаемого результата (когда в изогнутом состоянии контакт был, а в прямом контакт

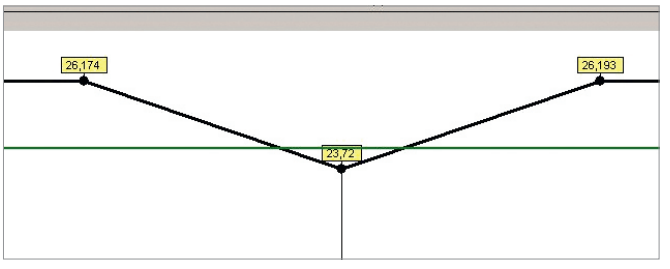

Рис. 1. Редкая флуктуационная ошибка при проведении самоконтроля, замеченная на конкретной КПА

отсутствовал) по проводу стал пропускаться ток 1 А. В плату аналогового ввода были выведены провода с резисторов, использующихся в роли нагрузки для создания такого тока.

При разгибании провода и работе ПО в фоновом режиме – регистрировался переходной процесс падения напряжения на нагрузке до 0 В. Процесс имеет вероятностный характер, зарегистрированы значения между номинальным напряжением 9,61 и 0 В: 9,179 и 0,012 В.

Был предпринят ряд попыток установить устойчивый контакт проводника с изломом в таком состоянии, когда излом забирает постоянно на себя часть напряжения. Удалось установить устойчивое состояние напряжения на нагрузке 9,1–9,2 В (потеря 0,41–0,31 В на изломе). Данное состояние удалось зафиксировать на протяжении 10 с.

Для самоконтроля КПА (регистрации недоразрывов) необходимо:

- уменьшение допуска нормы для сигналов с силовых проводников жгута;
- внедрение в механизм снятия данных с плат аналогового ввода проверки резкого изменения напряжения на канале – в момент снятия пачки данных для последующего усреднения;
- возможно, проведение самоконтроля КПА на вибростенде.

Пример неиспользования последнего пункта представлен на рис. 1, схематически изображающем поведение сигнала, снятого с одной из КПА. Такая ошибка возникала один раз в 25–50 тестов, при повторном тесте ошибка исчезала. Это придавало ошибке статус несущественной (самоконтроль проводится однократно раз в 3 года) – в итоге аппаратура была поставлена заказчику, а вопрос о необходимости выявления маловероятной ошибки самоконтроля остался. В инструкцию для страховки был приписан абзац вида: «тест считается ошибочным, если он показал ошибку два раза подряд».

Вероятные причины данной ошибки в контексте полученной информации с тестового стенда:

- недоразрыв проводника;
- выход за допуски сигнала, результат теста «не норма» – везение. Напряжение просело от нагрузки до значения 26,174 В вместо 27 В. Далее в результаты

для расчета среднего значения попало одно околонулевое значение при девяти корректных (среднее при одном нулевом значении – 23,56 В). Усредненный результат вышел за нижний предел –10% от 27 В.

ГЛУБОКОЕ ТЕСТИРОВАНИЕ ПЛАТ АНАЛОГОВОГО ВВОДА (ДОПОЛНИТЕЛЬНО К МАТЕРИАЛАМ, ПРИВЕДЕННЫМ В [3])

Обоснование данного пункта лежит в практике обнаружения ухудшения качества изготовления плат аналогового ввода PCI-9113A и, как следствие, отказа от их использования в будущих КПА.

Найденные проблемы:

- влияние каналов друг на друга. При подаче напряжения на канал № 0 появляется напряжение на канале № 1, иногда затрагивая и канал № 2. Исправлялось в ПО самоконтроля КПА и входного контроля ИСУ путем вычета из каналов паразитных напряжений. От платы к плате – номиналы паразитного напряжения различны. Данная проблема присутствует во всех платах;
- невозможность точно откалибровать плату, используя ее инструкцию по эксплуатации, п. 6.1.2 [16]. В части плат диапазон регулирования калибровочных потенциометров заканчивался, не приводя к достижению нужного результата. Платы, в зависимости от некорректного потенциометра, смещали реальное значение напряжения в ту или иную сторону. От платы к плате – могут быть проблемы с разными резисторами. Такую проблему имеют все платы PCI-9113A с 2014 года;
- плавающее внутреннее сопротивление канала, в зависимости от нагрузки, подключенной к каналу. Наименьшее зафиксированное значение – 80 кОм. От платы к плате – номиналы внутреннего сопротивления различны. Все платы имеют такую проблему.

ЗАКЛЮЧЕНИЕ

Длительная отработка использовавшихся методов углубления самоконтроля КПА привела к их уточнению и дополнению, а также к разработке новых методов углубления самоконтроля КПА и ПО в его составе.

ЛИТЕРАТУРА

1. **Белов С.** Углубление самоконтроля контрольно-проверочной аппаратуры изделий систем управления: однократные и многократные тесты плат расширения // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2022. № 4. С. 120–123.
2. **Белов С.** Углубление самоконтроля контрольно-проверочной аппаратуры изделий систем управления: расширение областей контроля // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2022. № 5. С. 88–92.
3. **Белов С.** Углубление самоконтроля контрольно-проверочной аппаратуры изделий систем управления: самоконтроль плат аналогового ввода до конечной сборки аппаратуры // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2022. № 6. С. 94–98.
4. Advantech. PCL-730. 32-ch isolated digital I/O ISA cards. User's manual / Taiwan, Taipei: Advantech Co., Ltd., 2012. P. 18.
5. Advantech. Model PCL-720. Digital I/O & Counter Card. User's manual/Taiwan, Taipei: Advantech Co., Ltd., 1990. 4.1. Register Structure and Format.
6. **Белов С. П.** Открытие портов ввода / вывода в Windows XP и выше (07.08.2014). М.: личный сайт, 2020. [Электронный ресурс] URL: https://bad-good.ru/2014/august/xp-ports.html.
7. **Белов С. П.** Получение статуса подключения к ЛВС (27.08.2019). М.: личный сайт, 2020. [Электронный ресурс] URL: https://bad-good.ru/2019/august/check-connect-lan.html.
8. **Белов С. П.** Разработка методики привязки программного обеспечения к комплектующим автоматизированного рабочего места без использования инсталлятора. М.: ФГБОУ ВПО Московский государственный университет приборостроения и информатики. Сборник научных трудов «Мехатроника. Робототехника. Автоматизация», 2014, № 7.
9. **Белов С. П.** Нестандартное использование классов и свойств Windows Management Instrumentation для привязки программного обеспечения к комплектующим автоматизированного рабочего места без использования инсталлятора // Мир науки. 2014. № 4 (6).
10. Свидетельство об официальной регистрации программы для ЭВМ № 2014660899 (Защитник ПО v.1.0). Программа предназначена для привязки программного обеспечения к конкретным комплектующим системного блока (посредством создания и использования зашифрованных ключей) / Белов С. П. 2014 г.
11. **Белов С. П.** Windows XP и реальное время (23.06.2020). М.: личный сайт, 2020. [Электронный ресурс] URL: https://bad-good.ru/2020/june/windows-xp-realtime.html.
12. **Белов С. П.** Тестер PCI-1713x v.1.3.0.0. М.: личный сайт, 2020. [Электронный ресурс] URL: https://bad-good.ru/programs.html#pci-1713_test.
13. **Речицкий А.** ОС Windows XP официально мертва, теперь окончательно. Ставрополь: Хабр, 2019. [Электронный ресурс] URL: https://habr.com/ru/post/449814.
14. **Белов С. П.** Проходник между жгутом и платой v.1.1 FINAL (21.04.2018). М.: личный сайт, 2018. [Электронный ресурс] URL: https://bad-good.ru/2018/april/mediators-db9-db50.html.
15. **Белов С. П.** Тестер БП ПК v.2.0 (23.10.2019). М.: личный сайт, 2019. [Электронный ресурс] URL: https://bad-good.ru/2019/october/tester-bp-pk-2.html.
16. ADLINK. NuDAQ PCI-9113A. 32 Channels Isolated Analog Input Card. User»s Guide/Taiwan, Taipei: ADLINK Technology Inc., 2003. P. 81.

Современные средства измерений

РАСШИРЕНИЕ ЧАСТОТНОГО ДИАПАЗОНА

Анализаторы спектра серии АКИП-4214

Диапазон частот

9 кГц... 13,6 ГГц
9 кГц... 26,5 ГГц

Уровень собственных шумов

165 дБм

Плотность фазовых шумов

-105 дБм/Гц@1 ГГц отстройка 10 кГц

Генераторы ВЧ-сигналов серии АКИП-3211

Диапазон частот

9 кГц... 13,6 ГГц
9 кГц... 20 ГГц

Выходной уровень

-130 дБм... 25 дБм

Плотность фазовых шумов

120 дБм/Гц @ 1 ГГц отстройка 20 кГц

Модуляция AM/ FM/ PM в стандартной комплектации

prist.ru

У ТОЧНОСТИ ЕСТЬ ИМЯ! ПРИСТ

119071, **г. Москва**, 2-й Донской пр., д. 10, стр. 4; тел.: +7 (495) 777-5591; prist@prist.ru
196006, **г. Санкт-Петербург**, ул. Цветочная, д. 18, лит. В, офис 202; тел.: +7 (812) 677-7508; spb@prist.ru
620089, **г. Екатеринбург**, ул. Цвиллинга, д. 58, офис 1; тел.: +7 (343) 317-3999; ek@prist.ru