УДК 656.052: 004.056

АРХИТЕКТУРА И ПРИНЦИПЫ РЕАЛИЗАЦИИ АППАРАТУРЫ СОПРЯЖЕНИЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Фурман И. А.[1], Малиновский М. Л.[2], Караман Д. Г.[3]

[1]Харковский национальный технический университет сельского хозяйства имени Петра Василенко,
[2]Публичная компания Thales group (Франция),
[3]ООО Научно-производственное предприятие "Стальэнерго" (г. Харьков)

Рассмотрены принципы построения аппаратуры сопряжения систем, имеющих различные протоколы обмена данными, архитектуру и идеологию обеспечения безопасности, обеспечивая при этом выполнение требований по надежности и безопасности на уровне увязки.

Постановка проблемы. Зачастую в создании современных сложных информационно-управляющих систем участвуют несколько компаний-разработчиков. Каждая компания реализует отдельную подсистему, которая взаимодействует с другими подсистемами через один или несколько интерфейсов в соответствии с некоторым алгоритмом и протоколом обмена. Требования к безопасности систем жестко регламентированы отраслевыми, государственными и международными стандартами [1]. В то же время у каждой компании-разработчика в арсенале имеется свой особый набор методов и средств реализации этих требований. В связи с широким многообразием методов и средств, применяемых различными компаниями для обеспечения безопасности, возникает необходимость решения сложных задач сопряжения (увязки) подсистем различных производителей.

Анализ последних исследований и публикаций. Затраты на разработку средств сопряжения зачастую соизмеримы с затратами на разработку тех систем, увязку которых необходимо выполнить. Для минимизации затрат компании-партнеры нередко идут на временные решения и оставляют релейные средства для увязки [2], в результате чего не достигается одна из важнейших целей модернизации – исключение электромеханических реле, требующих периодического обслуживания. Существует два подхода к решению обозначенной проблемы. Первый заключается в разработке и внедрении единых стандартов построения интерфейсов систем, связанных с безопасностью [3]. Этот подход требует вложения колоссальных материальных ресурсов и временных затрат на переработку архитектуры систем и протоколов обмена данными от всех участников рынка. Второй путь состоит в разработке универсальных средств сопряжения, позволяющих путем гибкого конфигурирования встроенного программного обеспечения настроить их на взаимодействие двух и более систем [4].

Цель статьи. В статье предложены основные результаты теоретических исследований и последующего применения на практике основополагающих принципов создания универсальных средств сопряжения информационно-управляющих систем и исполнительных механизмов релейно-механического типа, создаваемых и поддерживаемых различными компаниями-разработчиками и имеющих различную идеологию и методы обеспечения безопасности.

Основные материалы исследований. Обеспечение безопасности функционирования информационно-управляющей системы может осуществляться сразу на нескольких уровнях: уровне аппаратного обеспечения и устройств обработки данных, уровне информационного обмена и функционально-логическом уровне. На уровне аппаратного обеспечения и устройств обработки данных применяются различные варианты методов функционального и тестового диагностирования, резервирование методом дублирования, включение по мажоритарным схемам.

В промышленной автоматике для характеристики резервированных узлов управления сложилась своя система обозначений, описываемая общим правилом NooM, где N — предельное число элементов, при котором система будет оставаться работоспособной, а M — общее число резервированных элементов. Литера "D" в конце формулы будет означать наличие в системе встроенных диагностических средств, позволяющих своевременно обнаруживать и изолировать сбои, которые могут привести к опасным отказам. Простейшим методом повышения безопасности функционирования является дублирование ответственных подсистем со схемой резервирования 1oo2. При использовании дублирования основной экземпляр ответственной подсистемы включается параллельно с дублирующим, который может быть или копией первого, или дивергентным функциональным аналогом. Другая широко распространенная схема – с двойной кратностью 2oo3, при которой вместе с одним основным элементом включаются два дополнительных. Такой способ позволяет организовать простейшую систему голосования, основанную на принципах мажоритарности. В системах с повышенными требованиями к безопасности широко применяются различные виды диагностических средств. Наиболее востребованным является функциональное диагностирование, при котором сбои могут быть обнаружены и должным образом обработаны оперативно в течение всего времени функционирования системы. Однако в последнее время, в связи с повышением производительности вычислительных средств, на основе которых построены информационно-управляющие системы, появилась возможность проведения тестового диагностирования ответственных узлов за интервалы времени в итерациях рабочего цикла, пока они простаивают. В некоторых случаях, например, при тестировании работоспособности эле-

ментов памяти, применяются методы неразрушающего контроля. На уровне информационного обмена применяются контроль целостности данных с помощью вычисления контрольных сумм или методами помехоустойчивого кодирования, многократный повтор отправки, отправка данных по альтернативным каналам связи.

Практически во всех протоколах обмена данными по каналам связи промышленного назначения предусмотрены механизмы контроля целостности передаваемых данных с помощью контрольных сумм, вычисляемых для каждого передаваемого пакета или кадра. Обычно длина контрольной суммы составляет 8 или 16 бит (1 или 2 байта) в зависимости формата представления данных. Наиболее распространенными видами контрольных сумм в телекоммуникационных сетях общего и специального назначения являются CRC-8-CCITT, CRC-16-CCITT и CRC-32. Существуют и отраслевые стандарты построения контроля целостности, например, CRC-7-MVB, используемый в коммуникационных сетях поездного оборудования (MVB) и для связи с системами управления поездов (TCN) [5, 6]. Он же включен в стандарт IEC 60870-5 [7], в котором описан протокол передачи простых сообщений для удаленного контроля в распределенных информационно-управляющих системах.

Коды обнаружения и исправления ошибок применяются редко, поскольку их использование приводит к существенной избыточности ресурсов и снижению производительности. На функционально-логическом (алгоритмическом) уровне осуществляется контроль последовательностей выполнения операций, контроль времени выполнения операций, использование детерминированных автоматных моделей с необратимыми защитными состояниями.

Функционирование управляющей системы произвольной сложности можно описать конечноавтоматной моделью. Такая модель подразумевает определенный конечный набор состояний, в которых может пребывать система. Переход между состояниями определяется четкими правилами, а это значит, что всегда можно определить новое состояние, в которое перейдет система из текущего состояния.

Кроме того, типовая архитектура построения систем реального времени определяет однозначную, часто, цикличную последовательность смены состояний [8]. Таким образом, если на алгоритмическом уровне предусмотреть контроль смены состояний системы, то можно предупредить опасные последствия, если порядок смены был нарушен. Помимо цикличности в управляющих системах реального времени предусматривается и четкое ограничение длительности цикла [9]. Каждой операции выделяется свой временной слот, в течение которого должны быть выполнены все требуемые действия. Если временной лимит превышен, может произойти рассогласование сопряжения управляющей и исполнительной систем, что, в свою очередь, может привести к опасным последствиям. Контроль времени выполнения операций обычно производится с помощью автономных сторожевых таймеров, переполнение таймера является сигналом к приостановке системы и переводу ее в безопасный режим.

Архитектура и принципы реализации аппаратуры сопряжения. Аппаратура сопряжения (АС) представляет собой цифровую систему сбора, обработки и передачи информации через цифровой интерфейс и предназначена для увязки систем управления ответственными технологическими процессами и имеющих различную идеологию и методы обеспечения безопасности. Одним из частных применений АС является применение в составе цифрового модуля контроля рельсовых цепей (ЦМ КРЦ) в системах железнодорожной автоматики для обеспечения обмена данными между управляющей системой (УС) и объектными контроллерами (ОК).

При проектировании АС была разработана концепция обеспечения безопасности, которую можно охарактеризовать следующими положениями:

1) одиночный отказ аппаратных средств не должен приводить к возникновению опасного состояния;

2) одиночные отказы аппаратных средств, накопление которых, может привести к опасным последствиям, должны обнаруживаться и блокироваться;

3) сочетание одиночных отказов аппаратных средств не должно приводить к возникновению опасного состояния с интенсивностью, превышающей норму интенсивности опасных отказов.

Разработчиками предусмотрены следующие меры по обеспечению требуемых норм безопасности:

1) аппаратная избыточность;

2) проведение тестового самодиагностирования канала с помощью сверки сигнатур ответственных программных модулей аппаратуры АС независимо от наличия или отсутствия обмена данными между УС и ОК;

3) проведение функциональной самодиагностики аппаратуры АС путем непрерывного сравнения формируемых выходных данных;

4) применение комплектующих изделий с известными характеристиками качества.

В табл. 1 приведены ключевые характеристики систем, увязка которых выполняется при помощи АС при ее применении в составе ЦМ КРЦ. Из таблицы видно, что идеология построения увязываемых систем имеет фундаментальные отличия. В состав АС входят четыре специализированных вычислителя — Ядра логики (ЯЛ), которые образуют двухканальную четырёхмодульную структуру со схемой резервирования 1oo2D, и два Концентратора связи верхнего уровня (КСв), обеспечивающие связь между ЯЛ и ОК (рис. 1). Безопасность обмена данными между УС и АС основана на передаче информации по мажоритарной схеме "2oo3" с использованием контрольных сумм CRC-32. Структура взаимосвязей между УС и АС приведена на рис. 2. Каждая из подсистем УС – У1, У2, У3 – формирует четыре пакета управляющих данных, защищенных на прикладном уровне 32-разрядной контрольной суммой, для каждого из модулей АС. Благодаря синхронизации полученных данных между вычислительными модулями одного канала и между каналами по внутренним линиям связи достаточно получения непротиворечивых пакетов хотя бы от двух подсистем УС двумя модулями одного из каналов (четыре пакета), для того, чтобы данные считались корректными и были приняты в обработку.

В ответ на пакеты с управляющими воздействиями от каждого модуля АС формируются пакеты контрольной информации. Каждый пакет на прикладном уровне защищен 32-разрядной контрольной суммой. Для того чтобы данные об объекте управления считались достоверными, необходимо, чтобы как минимум две подсистемы УС получили корректные пакеты как минимум от двух разноименных модулей (А и В).

Таблица 1 – Ключевые характеристики систем, увязываемых с помощью АС

Характеристики	ЦМ КРЦ	Управляющая система
Архитектура резервирования	1oo2D (два дублированных канала)	2oo3 (два из трех)
Интерфейс	RS422	Ethernet
Время цикла	0,1 с	1 с
Критерий ухода в защитное состояние	Несовпадение контрольных сумм (тестовое диагностирование) либо выходных управляющих воздействий (функциональное диагностирование) хотя бы в одном цикле	Несовпадение результатов обработки данных в 3 и более циклах из 10
Критерии блокирования обмена данными со стороны смежной системы	Отсутствуют	Несовпадение данных в 3 и более циклах из 10

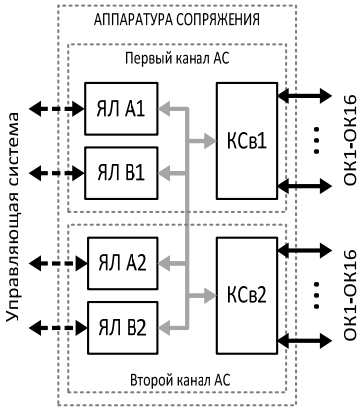

Рисунок 1 – Структурная схема АС

При потере связи с УС, АС сохраняет работоспособное состояние и транслирует приказы безопасного режима работы на ОК. Каждый канал АС может находиться в "работоспособном", "безопасном" или "защитном" состоянии. Переход каналов АС в безопасное состояние происходит при возникновении самоустраняющихся сбоев и перемежающихся неисправностей, которые можно устранить сбросом прикладных данных или встроенного программного обеспечения. Канал АС переходит в защитное состояние при обнаружении перманентных и неустраняемых отказов, обнаруженных в процессе функционального или тестового самодиагностирования.

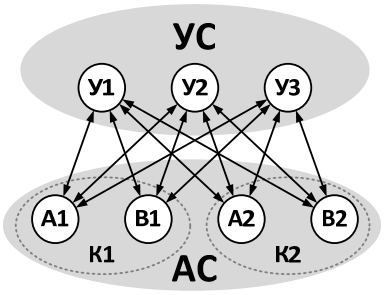

Рисунок 2 – Структура взаимосвязей между АС и УС

АС может работать в одноканальном режиме работы, когда функционирует только одна из пар вычислителей (А1-В1 или А2-В2) и в двухканальном режиме работы по схеме резервирования "1oo2D", когда параллельно функционируют обе пары вычислителей. Если АС работает в двухканальном режиме, то при уходе соседнего канала в защитное или безопасное состояние, предусмотрен автоматический переход в одноканальный режим работы по факту отсутствия межканальной связи. Встроенные средства самодиагностирования аппаратуры сопряжения осуществляют тестовое диагностирование на аппаратном уровне всех ответственных компонентов. Тестовое самодиагностирование выполняется в процессе функционирования вычислителя, для чего в главной циклограмме его работы выделен отдельный временной слот. Проверка ответственных модулей осуществляется путем подачи исчерпывающего набора тестовых воздействий. В процессе тестирования производится свертка реакций каждого проверяемого модуля в отдельную сигнатуру с помощью CRC-16, которые затем сравниваются с аналогичными сигнатурами соседнего ЯЛ. В случае несовпадения сигнатур, канал АС, в одном из вычислителей которого обнаружена неисправность, переводится в защитное состояние.

Структура внутренних взаимосвязей между вычислителями АС приведена на рис. 3.

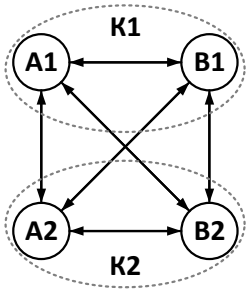

Рисунок 3 – Структура внутренних взаимосвязей АС

Такой способ организации обмена информацией называется "каждый со всеми" и позволяет значительно повысить устойчивость АС к отказам и искажениям в каналах связи между АС и УС, АС и ОК путем перегрузки и выравнивания прикладных и сервисных данных, а также безопасность работы вычислителей АС путем обмена сигнатурами самодиагностики. Структура взаимосвязей внутри АС, которая обеспечивает надежный обмен между ОК и АС, приведена на рис. 4.

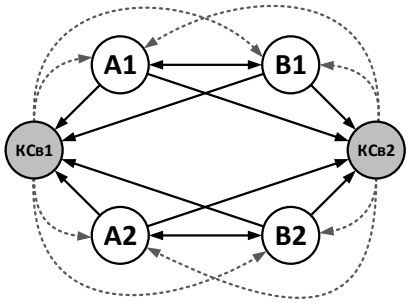

Рисунок 4 – Структура связей между АС и ОК (через КСв)

Обмен данными между АС и ОК организуется посредством двух специализированных концентраторов-коммутаторов КСв1 и КСв2, дублирующих друг друга. Безопасность обмена данными между АС и ОК обеспечивается с помощью двукратной отправки данных в виде двух специальным образом сформированных телеграмм, каждая из которых защищена с помощью восьмиразрядной контрольной суммы. При потере связи с ОК, АС транслирует в УС контрольную информацию с признаками неисправности ОК.

Практическая апробация. Разработанная Аппаратура сопряжения нашла применение при увязке Цифрового модуля контроля рельсовых цепей ЦМ КРЦ с системами централизации:

1) компании "Бомбардье" – более чем на 50 объектах в 5 странах;

2) компании "РАДИОАВИОНИКА" - на станции Вырица Российских железных дорог;

3) с релейными системами централизации Харьковского, Петербургского и Московского метрополитенов.

Выводы. В статье предложено техническое решение проблемы увязки подсистем в составе информационно-управляющих комплексов, создаваемых и поддерживаемых различными компаниями-разработчиками и имеющих различную идеологию и методы обеспечения безопасности. Выполнен анализ ключевых особенностей и отличий методов обеспечения безопасности в различных системах управления, связанных с безопасностью. Приведен пример реализации аппаратуры сопряжения, таких систем. Описанная аппаратура сопряжения нашла широкое применение при увязке Цифрового модуля контроля рельсовых цепей с различными системами железнодорожной автоматики.

Список использованных источников

1. IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES). Part 4. [Электронный ресурс] / International Electrotechnical Committee, Geneva. – 1999. – Режим доступа: http://www.iec.ch/functionalsafety. – 07.10.2017.

2. Фурсов С. И. МПЦ EBILock 950 – эволюция системы [Электронный ресурс] / С. И. Фурсов // "Автоматика, связь, информатика". – 2011. – Vol. 5. – с. 4-7. – Режим доступа: http://ru.bombardier.com/ru/pdf/press_article_pag4-7.pdf. – 07.10.2017 г.

3. Ulrich Maschek. Sicherung Des Schienenverkehrs: Grundlagen Und Planung Der Leit – Und Sicherungstechnik – Überarbeitete und erweiterte Auflage. [Электронный ресурс] / Ulrich Maschek // Springer Vieweg. – Wiesbaden, 2015. – p. 332. – Режим доступа: http://rcswww.urz.tu-dresden.de/~umaschek/estw/estw2.htm. – 07.10.2017 г.

4. Оффициальный сайт компании Радиоавионика, раздел "УСТРОЙСТВА ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ" [Электронный ресурс] / ОАО "Радиоавионика". – Режим доступа: http://www.radioavionica.ru/activities/ustroystva-zheleznodorozhnoy-avtomatiki-i-telemekhaniki/sistema-ets-em/163/. – 07.10.2017 г.

5. Hubert Kirrmann, Pierre A. Zuber. The IEC/IEEE Train Communication Network [Электронный ресурс] / Hubert Kirrmann, Pierre A. Zuber : IEEE Micro. March–April 2001. – p. 81–92. – Режим доступа: http://www.dca.ufrn.br/~affonso/DCA_STR/trabalhos/rt-diversos/The IEC-IEEE train communication network.pdf. – 07.10.2017 г.

6. IEC 61375. Train Communication Network. [Электронный ресурс] / International Electrotechnical Committee, Geneva. – 1999. – Режим доступа: http://www.iec-tcn.org. – 07.10.2017 г.

7. Clarke, Gordon R.. Practical modern SCADA protocols: DNP3, 60870.5 and related systems. [Текст] / Gordon R. Clarke, Deon Reynders. – Newnes, 2004. – 544 p.

8. Laplante, Phillip A. Real-Time Systems Design and Analysis: Tools for the Practitioner. [Текст] / Phillip A. Laplante, Seppo J. Ovaska. – John Wiley & Sons, 2011. – 560 p.

Анотація

АРХІТЕКТУРА І ПРИНЦИПИ РЕАЛІЗАЦІЇ АПАРАТУРИ СПОЛУЧЕННЯ СИСТЕМ, ПОВ'ЯЗАНИХ З БЕЗПЕКОЮ

Фурман І. О., Малиновський М. Л., Караман Д. Г.

Розглянуто принципи побудови апаратури сполучення систем, що мають різні протоколи обміну даними, архітектуру і ідеологію забезпечення безпеки, забезпечуючи при цьому виконання вимог до надійності і безпеки на рівні ув'язки.

Abstract

ARCHITECTURE AND IMPLEMENTATION PRINCIPLES OF DATA EXCHANGE EQUIPMENT FOR SAFETY RELATED SYSTEMS

I. Furman, M. Malinovsky, D. Karaman

Principles of construction data exchange equipment between systems having different communication protocols, architecture and safety assurance ideology, while ensuring compliance with the requirements for reliability and safety at the level of alignment are given.