КРАТКИЙ ОБЗОР *LON*-СОВМЕСТИМЫХ СИСТЕМ ОХРАННОЙ СИГНАЛИЗАЦИИ И КОНТРОЛЯ ДОСТУПА

Г. Латышев
ООО «Квантум-С»

Сегодня на рынке систем автоматизации преобладают системы закрытого протокола. Так производитель пытается защититься от хакеров элементарным сокрытием полного описания процесса взаимодействия компонент системы между собой. Ситуация выглядит примерно так: пользователь спрашивает «Реализована ли аутентификация отправителя сообщения на уровне протокола в Вашей системе?» и получает ответ «Протокол засекречен, на Ваш вопрос ответить не можем». Конечно, огульно заявлять, что производители скрывают простой факт что «король то голый» нельзя. Срабатывает простой принцип презумпции невиновности. Однако гораздо больше доверия вызывает производитель, использующий открытый протокол совместно с надежными механизмами защиты данных и аутентификации. Наиболее подходящим для систем безопасности является протокол Lonworks, поэтому темой данной статьи является попытка провести анализ рынка систем безопасности применительно этого протокола.

О протоколе Lonworks слышали многие, однако вкратце напомним еще раз о том, что же он собой представляет:

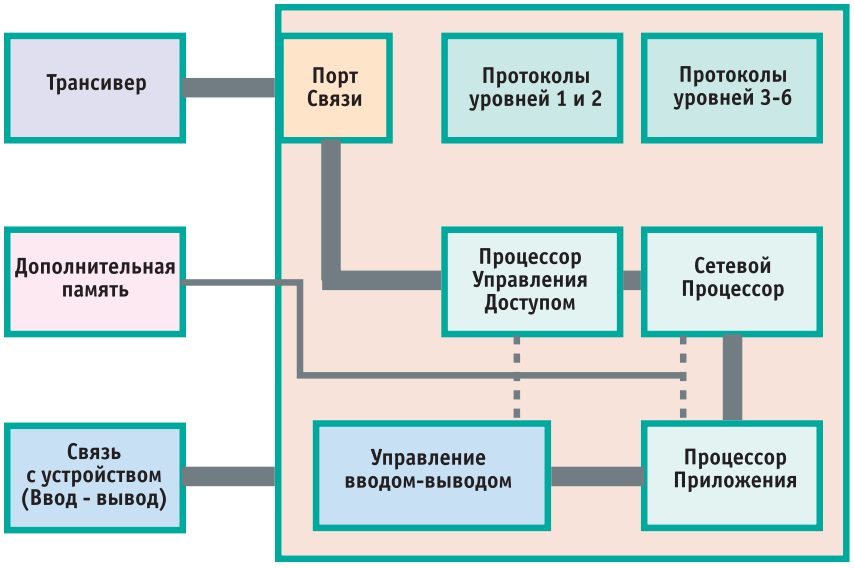
- разработана компанией Echelon Corporation в 1990 году;
- технология является стандартом «де факто» для сетей контроля, поддерживается более 3000 производителей оборудования;
- в данный момент принят комитетом Electronic Industry Assotiation (EIA) как стандарт EIA/IS-709;
- соответствует семиуровневой модели ISO и поддерживает все 7 уровней;
- обеспечивает решение проблем разработки, построения и обслуживания СКУ любого масштаба и назначения;
- включает в себя инструменты проектирования, устройства, протоколы взаимодействия, инструменты управления сетью, форматы данных, техническую поддержку.

В основе реализации лежит специализированная микросхема Neuron Chip, содержащая три микропроцессора с общей разделяемой памятью. Каждый из указанных микропроцессоров специализируется на своей подзадаче:

- Обеспечение процесса измерения и контроля (сигнальный процессор) посредством аппаратных аналоговых и дискретных входов/выходов.
- Реализация прикладного алгоритма (реализация алгоритма управления технологическим процессом).
- Обеспечение обмена информацией по специализированному протоколу передачи данных Lontalk, разработанному специально для решения задач автоматизации и безопасности.

Микросхема Neuron (*рис. 2.*) изобретенная компанией Echelon Corporation в 1990 году, и являющаяся краеугольным камнем всей технологии LonWorks, содержит на самом деле три процессора. На рисунке вы можете видеть структурную схему этого кристалла (*рис. 1.*).

Рис. 1. Структурная схема кристалла микросхемы Neuron



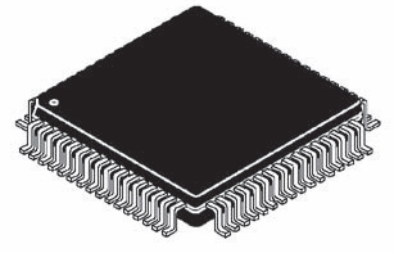


Рис. 2. Микросхема Neuron

Модель MC143150B1FU1, выпускаемая фирмой Motorola, имеет:

- Три 8-битных процессора конвейерной архитектуры для одновременной обработки кода приложения и сетевых пакетов.
- Программируемый 11-ти контактный порт ввода/вывода, имеющий 34 режима работы.
- Два 16-ти битных таймера/счетчика.
- 5-ти контактный коммуникационный порт для подключения сетевого трансивера.
- 2 Кб статической ОЗУ.
- 512 байт флэш памяти и встроенный накристальный преобразователь напряжения для ее перепрограммирования.
- 48-битный идентификационный серийный номер, уникальный для каждого кристалла.
- Энергопотребление 16ma на частоте 10 Mhz, 4 ma на частоте 625 Khz и 15 μa в энергосберегающем режиме.
- Позволяет адресовать до 64Кб внешней ОЗУ(16 из них необходимы для реализации протокола LonWorks).

Несмотря на то, что протоколу уже 16 лет, он не устаревает и сейчас. И главная причина этому – отсутствие реального конкурента «трехголовому монстру» Neuron Chip-а. В тех случаях, когда ресурсов микросхемы не хватает, используется так называемая Host архитектура, когда Neuron Chip работает в паре с более мощным процессором и памятью. Именно такая архитектура наиболее подходит для реализации решений задач безопасности.

Приведем конкретные количественные показатели по наиболее популярным в мировой практике открытым протоколам передачи данных в сетях автоматики *(см. табл. 1.)*.

Без ограничения общности можно сказать, что в большинстве представленных на отечественном рынке систем пре-

обладают протоколы на базе RS485. В приведенной выше таблице нет колонки для RS485, но любой специалист без труда заполнит ее.

Но главная «изюминка» протокола Lonworks, делающая его уникальным с точки зрения задач обеспечения безопасности – это аутентификация отправителя сообщения на «сеансовом» уровне семиуровневой модели OSI/ISO. Таким образом, в Lonworks решена проблема «компрометирующего воздействия».

Следующее кардинальное преимущество Lonworks – легкость интеграции с системами вентиляции, отопления, кондиционирования, управления освещением и диспетчеризацией. Конечно, при условии что эти системы используют либо Lonworks, либо другой открытый протокол, имеющий шлюз на Lonworks. Однако сегодня смело можно утверждать, что во многих случаях крупный корпоративный Заказчик явно указывает в своем Техническом Задании Lonworks как основной протокол автоматизации объекта.

Существенным фактором в пользу Lonworks является реализация по-событийного обмена информацией, реализованного аппаратно в самом Neuron Chip. Это означает, что контроллер будет высылать значение измеряемого параметра, только если он изменился. Данный прием позволяет многократно увеличивать количество «точек контроля» системы не перегружая сеть передачи данных.

Итак, зададимся вопросом, что именно должен реализовать добросовестный производитель, решившийся осчастливить рынок системой СКД на открытом протоколе Lonworks. Изложим требования по пунктам:

1. Поддержка стандартных считывателей тач-мемору, магнитных, смарт-карт, проксимити-карт. Лучше всего если поддерживается интерфейс Wiegand. Так можно обеспечить максимальную совместимость со считывателями наиболее популярных производителей.
2. Контроллер считывателя должен поддерживать не менее 2-х считывателей. Это необходимо для снижения стоимости решения.
3. Контроллер считывателя должен иметь достаточный объем энергонезависимой памяти для хранения базы данных по проходам.
4. В системе должна быть реализована постоянная проверка (тестирование) всех сетевых устройств на работоспособность и отсутствие сбоев в работе оборудования и целостности данных.
5. Система должна быть максимально децентрализована. В идеале каждый считыватель должен иметь внутри себя полную версию базы данных по проходам на все здание. Нежелательно применение персонального компьютера в цепи принятия решения по разрешению прохода. Это во-первых, увеличивает время реакции системы, а во-вторых, сильно снижает уровень надежности системы в целом.
6. Система должна иметь защиту от двойного пасбэка, реализованную на уровне контроллеров считывателей.
7. Все сетевые обмены должны быть только с включенной аутентификацией. Все данные передаются по сети только в зашифрованном виде. Ключи должны меняться регулярно. Желательно применить

Табл. 1. Количественные показатели по наиболее популярным в мировой практике открытым протоколам передачи данных в сетях автоматики

ХАРАКТЕРИСТИКИ	BACnet	CAN-based (SDS, DeviceNet	CEBus	Fieldbus SP-50, Foundation Initiative.	LONWORKS
Область применения	Автоматизация зданий	Стандарт автоматизации (J1850,J1939) Дискретная автоматизация (SDS, DeviceNet)	Автоматизация жилища	Промышленные станки и приборы	Автоматизация зданий. Управление производством Автоматизация предприятий Транспорт Автоматизация жилища
Уровни OSI/ISO	1,2,3,7	1,2,7	1,2,3,7	1,2,7	1,2,3,4,5,6,7
Поддерживаемые среды передачи	Витая пара. Коаксиальный кабель. Оптоволокно.	Витая пара (SDS, DeviceNet). Альтернативные решения на основе оптоволокна для сетей CAN.	Силовые электрические линии (FCC) Коаксиальный кабель RF.	Витая пара H1, H2(1). Коаксиальный кабель H2 (2.5). Характерная безопасность передачи данных на скорости 31.25 Kbps и 1 Mbps.	Витая пара со свободной топологией с возможностью подачи питания. Характерная безопасность витой пары. Линии электропитания совместимые со стандартом FCC и CENELEC. Оптоволокно. Коаксиальный кабель RF (несколько диапазонов)
Схема доступа к среде передачи	CSMA/CD. Master/ slave, token passing. Удаленный доступ через модем.	CSMA/CR	CSMA/CD	Предопределенный централизованный планировщик с возможностью делегирования токена.	P-персистентный CSMA/CD. Дополнительный CSMA/CR. Возможность включения системы приоритетов.
Скорость передачи данных	10 Mbps	1 Mbps(CAN) 1 Mbps (SDS) 500 Kbps (DeviceNet)	6.666 kbps (или 10 kbps)	31.25 kbps для H1 1 Mbps для H2 (1) 2.5 Mbps для H2 (2.5)	До 1.25 Mbps.
Максимальное адресное пространство	2^{48}	2^7=128 (SDS) 2^6=64 (DeviceNet) 2^{11} (CAN 1) 2^{29} (CAN 2)	2^{16}	127 логических узлов в сегменте, 64 сегмента.	2^{48} доменов, 32000 узлов в домене.
Поддержка маршрутизаторов сетевого уровня	Есть	Нет	B-маршрутизаторы.	Есть. Поддержка различных скоростей маршрутизации.	Самообучающиеся или конфигурируемые маршрутизаторы. Хорошая реализация как физических, так и логических репитеров. Полная поддержка средствами инсталляции.
Безопасность (аутентификация)	Есть	Нет	На уровне приложения (ограничения сопряжимости)	Нет	Есть
Поддержка совместимости сетей	Определены объекты высокого уровня. Службы управления сетью не определены.	Определены объекты высокого уровня (SDS, DeviceNet). Служба управления сетью определена (SDS, DeviceNet). Не существует реализации теста на совместимость с DeviceNet. Сертификационный план определен для SDS и определяется для DeviceNet.	Определены высокоуровневые функции. Служба управления сетью не определена. Не существует теста на совместимость. Сертификационный план до сих пор не определен.	10 функциональных блоков определено, еще 20 определяется. Поддерживается соответствие с применяемым стеком протоколов. Сертификационный план до сих пор не определен.	Определены объекты высокого уровня и стандартные конфигурируемые параметры. Определена и реализована служба управления сетью. Тест на совместимость определен. Сертификационная программа определена.
Степень готовности	Спецификационный материал находится на конечной стадии разработки чернового варианта.	Спецификация DeviceNet часть 1 опубликована, часть 2 готовиться. Спецификация SDS опубликована.	Документы по CAN доступны. Спецификация по 'Interim' утверждена. Трансиверы для сетей электропитания, системы разработки и некоторые другие продукты доступны.	Документы + стек протоколов Q3'95. Документы по доступу к среде передачи и физическому интерфейсу: H1-сейчас, H2-Q3'95. В соответствии с реализацией тестов на совместимость Q3'95.	Доступны спецификации для всех протоколов, служб и системных интерфейсов. Документы доступны со времени выхода Q3'91. Доступно более 200 готовых блоков. Доступны средства разработки.

аппаратный прибор генерации ключей, позволяющий избежать регулярности в значениях разовых ключей.

8. Питание контроллеров должно осуществляться локально. Нежелательно использовать схемы питания от шины передачи данных (Lonwork LPT10) во избежание блокирования работы контроллера путем короткого замыкания шины.

9. При интеграции СКД с другими системами жизнеобеспечения в рамках концепции ИЗ, шлюзовые элементы не должны позволять реализовывать управляющие воздействия на систему СКД со стороны смежных систем (вентиляция, управление освещением, кондиционирование, отопление и т.д.).

10. Для предотвращения вывода из строя сетевых приемо-передатчиков контроллеров путем подачи высокого напряжения на шину передачи данных, необходимо использовать так называемые Overvoltage arresters (ограничители напряжения), подключаемые на каждом физическом сегменте шины.

11. Каждый физический сегмент шины должен быть терминирован согласно каноническим схемам по технологии Lonworks.

12. Нежелательно использовать сети общего пользования для передачи трафика системы СКД. В случае, если это происходит, необходимо обеспечить стойкое шифрование трафика и гарантированную полосу пропускания.

13. Доступ к активному оборудованию СКД должен быть строго разграничен. На всех шкафах, содержащих такое оборудование должны быть тамперы, фиксирующие факт открытия шкафа.

14. Желательно чтобы журнал тревог велся самим контроллером считывателей и хранился в его энергонезависимой памяти.

К сожалению ни у одного из присутствующих ныне на отечественном рынке производителей нет решения, удовлетворяющего всем вышеперечисленным требованиям. Скорее наоборот, проще перечислить типовые ошибки:

1. Контроллеры считывателей чаще всего совместимы лишь с узким перечнем считывателей, часто один контроллер рассчитан на работу всего с одним считывателем.

2. Часто производитель закрывает интегратору возможность использовать для инсталляции типовой софт (Lonmaker), навязывая фирменный программный пакет, имеющий заведомо более сокращенный функционал, в частности, не позволяющий включить аутентификацию.

3. Многие производители реализуют блок регистрации тревог как отдельный контроллер, однако при потере связи по сети, теряется протоколирование событий.

4. Наиболее именитые производители увлекаются использованием так называемого «механизма явных сообщений». Эта технология позволяет контроллерам обмениваться нетипизированными данными произвольной длинны. Так например, реализован BACNET поверх Lontalk. При этом инсталлятор не имеет инструментария для проверки защищенности обмена. Ввиду того, что производитель секретов не раскрывает, и специального инструментария не выдает, приходится констатировать закрытость решения.

5. Ни один производитель пока что не удосужился снабдить свое решение встроенным диагностическим инструментарием для сети. Поэтому инсталлятор пока что всегда должен позаботиться о себе сам, приобретая программно-аппаратные средства анализа трафика за свой счет.

Приведем несколько примеров:

Система охранной сигнализации и контроля доступа Apice (Эпиче). Набор предлагаемых компонент весьма скромен:

- Контроллер считывателя на один считыватель с Wiegand интерфейсом.
- Модуль контроля проходов (содержит базу данных по проходам).
- Интерфейсные модули шлейфов, клавишные панели и т.д.

Система реализована на Lonworks TP/FT10 со свободной топологией и может быть интегрирована в общий BMS здания.

Система охранной сигнализации и контроля доступа SECULON (Секьюлон). Набор компонентов более широк и включает:

- центральную панель системы, поддерживающую подключение до 4-х информационных магистралей;
- контроллеры считывателей на два считывателя;
- интерфейсные модули шлейфов, клавишные панели и т.д.;
- модуль подключения принтера;
- модуль подключения GSM модема.

Система использует Lonworks-RS485, что несколько затрудняет интеграцию в общую BMS здания.

Система охранной сигнализации и контроля доступа Timecon (Тимекон). Набор компонент аналогичен Apice.

Система охранной сигнализации и контроля доступа Итриум (Россия). Набор компонент гораздо больше, удачно решены задачи подключения стандартных считывателей, используется как стандартный, так и свой конфигурационный софт. Используется аутентификация. Однако модуль регистрации тревог выполнен отдельным контроллером. Система реализована на Lonworks TP/FT10 со свободной топологией и может быть интегрирована в общий BMS здания.

Выводы:

Lonworks имеет прекрасные перспективы к использованию на рынке систем безопасности ввиду наличия механизма аутентификации, простоте инсталляции, достаточной скорости передачи данных (78кбит или 1250кбит, витая пара сечением 0,8) в сочетании с высокой надежностью и отказоустойчивостью. Между тем, в крупных инсталляциях необходимы специалисты, имеющие высочайшую квалификацию в области самого протокола, дорогостоящие средства диагностики сетевого трафика. Ввиду недостаточной скорости передачи данных в Lontalk, не представляется возможным использовать непосредственно сети Lonworks для передачи видеоряда от камер наблюдения. Таким образом, в системах видеонаблюдения, Lonworks может использоваться только для управления аппаратурой видеонаблюдения. За последние два года номенклатура lon-совместимого оборудования доступного на Российском рынка увеличилась в два раза, что позволяет прогнозировать дальнейшее появление на рынке новых устройств. Будем надеяться что в следующем году подобный список «типовых недостатков» станет короче…