

УДК 004

**ОБЗОР ПРОМЫШЛЕННЫХ ПРОТОКОЛОВ СВЯЗИ ДЛЯ
ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ КОНТРОЛЛЕРОВ**

Кокташев А.С., студент(ка) гр. ИТб-221, IV курс

Научный руководитель: Ванеев О.Н., к.т.н., доцент

Кузбасский государственный технический университет имени Т.Ф.

Горбачёва,

г. Кемерово

Роль протоколов связи в архитектуре ПЛК. В современных системах автоматизации программируемый логический контроллер давно перестал быть изолированным устройством, работавшим только с локальными входами и выходами. Практически любой ПЛК сегодня должен обмениваться данными с удаленными станциями ввода-вывода, частотными преобразователями, сервоприводами, панелями оператора, SCADA, MES, историческими базами данных и облачными сервисами. Поэтому выбор протокола связи определяет не только скорость обмена, но и архитектуру всей системы: глубину диагностики, удобство ввода в эксплуатацию, масштабируемость, устойчивость к отказам и совместимость оборудования разных производителей. В отличие от офисных сетей, промышленная среда предъявляет к коммуникации особые требования: прогнозируемую задержку, низкий джиттер, устойчивость к электромагнитным помехам, возможность быстрого поиска неисправностей и длительную поддержку установленной базы оборудования. По этой причине эволюция сетей для ПЛК шла не по пути простой гонки за пропускной способностью, а по пути поиска разумного баланса между детерминированностью, стоимостью, открытостью и удобством эксплуатации [1].

Классификация и критерии выбора. Условно протоколы, применяемые рядом с ПЛК, можно разделить на три группы. Первая группа — классические последовательные и полевые сети, к которым относятся Modbus RTU, PROFIBUS и CANopen. Их сильные стороны — зрелость, предсказуемость и сравнительно низкая стоимость реализации. Вторая группа — промышленный Ethernet: PROFINET, EtherNet/IP, EtherCAT и близкие к ним решения. Здесь на первый план выходят высокая пропускная способность, короткие циклы обмена, возможность объединения больших распределенных систем и тесная интеграция с современными программными средствами. Третья группа — интеграционные и межсистемные протоколы, среди которых особое место занимает OPC UA, ориентированный не только на передачу значений, но и на описание их смысла. При выборе протокола важно оценивать не только номинальную скорость линии, но и время цикла, джиттер, поддерживаемые топологии, количество узлов, глубину диагностики, наличие механизмов резервирования, стандартизованные профили устройств, требования к кибербезопасности и соответствие экосистеме конкретного производителя. Исследования показывают, что даже сети с одинаковой физической скоростью могут давать разное качество управления из-за

различий в обработке кадров, механизмах синхронизации и сетевой организации [1, 15, 16].

Modbus RTU и Modbus TCP. Modbus остается одним из самых узнаваемых и распространенных протоколов в промышленной автоматизации. Он был разработан компанией Modicon еще в 1979 году и изначально ориентировался на обмен технологическими данными между устройствами промышленного управления. Принципиально важно, что Modbus в основном определяет уровень приложения, поэтому может использоваться поверх разных физических сред: EIA/TIA-232, EIA/TIA-485 и Ethernet через TCP/IP [2]. Это объясняет его долгую жизнь и огромную совместимую экосистему. Для простых задач Modbus очень удобен: структура кадров понятна, регистровая модель легко реализуется даже в недорогих устройствах, а RTU-режим остается более эффективным, чем ASCII, поскольку последний требует почти вдвое больше бит при той же полезной нагрузке [2]. В варианте Modbus TCP сохраняется знакомая модель регистров, но упрощается интеграция в Ethernet-инфраструктуру. Недостатки у этого семейства также хорошо известны: циклический опрос, ограниченная семантика данных, заметная зависимость от конкретной карты регистров производителя, а в исторически сложившихся внедрениях — слабая встроенная защита. Формально существует Modbus Security с TLS и X.509v3-сертификатами, однако в реальной промышленной базе поддержка этого расширения пока не столь универсальна, как хотелось бы [3]. Поэтому Modbus особенно уместен для счетчиков, датчиков, частотных приводов, несложных систем диспетчеризации и проектов модернизации, где важнее простота и совместимость, чем сверхмалые циклы обмена.

PROFIBUS DP/PA. PROFIBUS — это зрелая полевая сеть, которая сыграла огромную роль в развитии промышленной автоматизации и до сих пор сохраняет практическое значение в большом числе действующих производств. Для медного интерфейса RS485 поддерживаются скорости от 9,6 кбит/с до 12 Мбит/с [4], а типовая сегментная организация допускает до 32 узлов в сегменте [4]. В промышленном смысле PROFIBUS ценят за предсказуемый циклический обмен, устойчивую инструментальную базу, развитую культуру диагностики и большой парк совместимых устройств. На предприятиях, где много удаленных модулей ввода-вывода и давно эксплуатируемых шкафов управления, этот протокол нередко остается экономически оправданным решением. Дополнительным преимуществом является накопленная компетенция персонала: обслуживание и поиск неисправностей в PROFIBUS-сетях хорошо методически отработаны. Вместе с тем ограничения становятся все заметнее по мере роста требований к интеграции с ИТ-системами и к объему диагностических данных. По пропускной способности, гибкости топологий и удобству сопряжения с современными программными платформами PROFIBUS уступает семейству промышленного Ethernet. Поэтому сегодня его чаще выбирают не как универсальный стандарт для новых систем, а как

надежную основу существующей установленной базы, которую требуется сохранить при постепенной модернизации [1, 4].

PROFINET. PROFINET сегодня является одним из ключевых стандартов промышленного Ethernet в дискретной автоматизации. Согласно материалам PI, этот протокол обеспечивает обмен в реальном времени между промышленными устройствами, поддерживает различные топологии, а также предоставляет механизмы конфигурирования и диагностики [5]. На практике PROFINET интересен тем, что внутри одного семейства объединены разные уровни требований: RT подходит для большинства типовых задач автоматизации, тогда как IRT предназначен для жестко синхронизируемых приложений. В профиле PROFIdrive подчеркивается, что при скорости 100 Мбит/с и полном дуплексе PROFINET RT уже дает времена обновления шины, которые на несколько порядков лучше традиционных полевых сетей, а дополнительные механизмы Fast Forwarding, Dynamic Frame Packing и Fragmentation позволяют достигать циклов до 31,25 мкс в IRT-режиме [6]. Для задач высокой доступности важны и средства резервирования: PI отдельно описывает MRP как базовый механизм кольцевой избыточности и MRPD как бесшовную схему для быстрого изохронного обмена [7]. С инженерной точки зрения сильной стороной PROFINET является баланс: высокая скорость сочетается с богатой диагностикой, стандартизованными описаниями устройств и широкой производственной поддержкой. Слабая сторона — более высокая сложность проектирования по сравнению с Modbus, особенно если речь идет о больших сетях, управляемой инфраструктуре и синхронизируемых приводных системах [5-7].

EtherNet/IP. EtherNet/IP представляет собой другой путь развития промышленного Ethernet. По данным ODVA, он использует стандартный Ethernet IEEE 802.3 в сочетании со стеком TCP/IP и верхнеуровневым протоколом CIP [8]. Такая архитектура делает его особенно привлекательным там, где нужно не противопоставлять промышленную сеть корпоративной инфраструктуре, а максимально использовать привычные Ethernet-подходы. ODVA указывает поддержку различных скоростей интерфейсов — 10, 100 Мбит/с и 1 Гбит/с, а также возможность строить звезду, линию или Device Level Ring (DLR) [8]. Для задач синхронного управления важно расширение CIP Sync: оно основано на IEEE 1588 и допускает точность синхронизации между двумя устройствами менее 100 нс [9]. Не менее значимы и современные средства защиты: CIP Security обеспечивает аутентичность, целостность, авторизацию и, при необходимости, конфиденциальность трафика на базе TLS и DTLS [10]. Сильные стороны EtherNet/IP — естественная интеграция с обычной Ethernet-инфраструктурой, широкий набор объектных профилей CIP, развитые возможности включения в ИТ/ОТ-контур и зрелая экосистема в ряде вендорских платформ. Ограничения связаны с тем, что фактическая детерминированность сильнее зависит от сетевого дизайна, настроек коммутаторов, IGMP/multicast и дисциплины проектирования, чем в протоколах, изначально ориентированных на сверхкороткие циклы на уровне

кадра. Тем не менее как универсальный промышленный Ethernet для заводских систем он остается одним из наиболее сильных кандидатов [8-10].

EtherCAT. EtherCAT был разработан как высокопроизводительный промышленный Ethernet для задач, где критичны короткие циклы и очень точная синхронизация распределенных узлов. По материалам EtherCAT Technology Group, при его создании целевыми ориентирами были времена цикла не более 100 мкс и джиттер синхронизации не более 1 мкс [11]. Принцип работы EtherCAT отличается от классической коммутации кадров: устройства обрабатывают телеграмму «на лету», извлекая и вставляя свои данные по мере прохождения кадра через узел. Такая организация дает очень малую суммарную задержку и делает протокол особенно полезным для сервоприводов, многокоординатных механизмов, робототехники, испытательных стендов и систем точного позиционирования. Дополнительное преимущество дает механизм Distributed Clocks, благодаря которому результирующий джиттер в системе оказывается значительно меньше 1 мкс [11]. С практической точки зрения EtherCAT часто рассматривают как эталонное решение для hard real-time в пределах машинного уровня. Его слабая сторона не в скорости, а в том, что для многих несложных проектов такой уровень производительности избыточен: если система состоит из десятка дискретных датчиков, простых приводов и панели оператора, выигрыша от столь высоких характеристик может быть меньше, чем стоимость входа в соответствующую экосистему. Поэтому EtherCAT наиболее рационален там, где скорость и точная синхронизация действительно являются определяющими требованиями [11, 15].

CANopen. CANopen занимает особую нишу между классическими полевыми шинами и современными Ethernet-решениями. Организация CiA определяет его как CAN-основанную коммуникационную систему, развившуюся в стандартизованную встроенную сеть с высокой гибкостью конфигурации [12]. Первоначально CANopen был ориентирован на motion-oriented machine control, но затем получил широкое распространение в медицинском оборудовании, внедорожной технике, железнодорожных и морских приложениях, а также в распределенных встраиваемых устройствах [12]. Важным элементом архитектуры является object dictionary — словарь объектов, который связывает коммуникационную часть с прикладным уровнем и служит ключом к конфигурации и диагностике устройства [12]. Для передачи данных используются SDO, PDO, сетевое управление NMT и протоколы контроля ошибок. Еще одна сильная сторона CANopen — понятная зависимость длины линии от скорости: классическая таблица CiA показывает диапазон от 1 Мбит/с на 25 м до 10 кбит/с на 5000 м [13]. Это делает протокол удобным для компактных распределенных машин и мобильных систем, где важны простота электроники, предсказуемое поведение и относительно небольшие объемы трафика. Ограничения очевидны: по пропускной способности и масштабируемости CANopen уступает промышленному

Ethernet и хуже подходит для передачи больших диагностических потоков, данных машинного зрения и сложной межсистемной интеграции [12, 13].

OPC UA. OPC UA не является классическим полевым протоколом в узком смысле, однако для систем на базе ПЛК его значение настолько велико, что обходить его вниманием нельзя. OPC Foundation описывает OPC UA как платформонезависимую сервис-ориентированную спецификацию, объединяющую возможности OPC Classic и предлагающую более безопасный и масштабируемый путь обмена данными [14]. В отличие от простых регистровых протоколов, OPC UA переносит не только значения, но и их структуру, типы и контекст применения. Это особенно важно при объединении ПЛК, SCADA, MES, исторических баз и облачных сервисов. Безопасность встроена в саму модель: спецификация прямо указывает на аутентификацию клиентов и серверов, аутентификацию пользователей, контроль целостности и конфиденциальности обмена [14]. Дополнительную ценность создают Companion Specifications, которые задают единые информационные модели для конкретных отраслей и классов оборудования. При этом развитие PubSub и инициатив уровня Factory Automation расширяет область применения OPC UA в сторону низколатентного обмена и полевого уровня [14]. Однако в инженерной практике важно различать роли: классический клиент-сервер OPC UA крайне удобен для межсистемной интеграции и безопасного доступа к данным, но обычно не рассматривается как основной транспорт для жестких контуров управления с субмиллисекундными циклами. Поэтому его правильнее воспринимать как протокол верхнего и межуровневого взаимодействия, который дополняет, а не обязательно заменяет полевой Ethernet [14].

Сравнение протоколов по инженерным критериям. Сопоставляя промышленные протоколы связи для ПЛК, важно избегать упрощения вида «у кого выше Мбит/с, тот и лучше». Реальная эффективность сети управления определяется временем цикла, предсказуемостью задержек, глубиной диагностики, устойчивостью к единичным отказам, удобством замены устройства и качеством инструментальной поддержки. Именно поэтому сравнительные исследования промышленных Ethernet-протоколов подчеркивают, что EtherNet/IP, EtherCAT и PROFINET IRT дают различные характеристики в режиме реального времени, а значит — разное качество управления при одинаковой логике объекта [15]. С другой стороны, работы, рассматривающие связь между оборудованием и программным мониторингом, показывают, что при переходе от чистого управления к интеграции данных возрастает значение стандартизованных моделей, удобства извлечения информации и совместимости с аналитическими платформами [16]. По этой причине в реальном проекте часто используется не один, а несколько протоколов сразу. Например, быстрый контур сервоприводного движения может работать по EtherCAT, основная линия ввода-вывода — по PROFINET, вспомогательные датчики учета энергии — по Modbus TCP, а публикация данных в MES и архив выполняется через OPC UA. Такой многослойный

подход оказывается не признаком избыточности, а естественным следствием разных требований на разных уровнях автоматизации [1, 15, 16].

Профили, семантика и взаимозаменяемость устройств. На практике удобство протокола определяется не только способом передачи байтов, но и тем, насколько хорошо стандартизованы профили устройств и описания параметров. В Modbus одна и та же функция чтения регистров может использоваться тысячами устройств, но смысл конкретных адресов при этом задается производителем, поэтому инженеру приходится постоянно работать с картами регистров и таблицами соответствия. В CANopen важную роль играет словарь объектов, а в EtherNet/IP — объектная модель CIP и набор профили устройств. В экосистеме PI значительный эффект дают GSD-файлы, PROFIdrive, PROFIsafe и другие прикладные профили, благодаря которым замена компонента на аналог другого производителя становится более реалистичной. OPC UA идет еще дальше и переносит в сеть формализованное описание самих данных и их контекста через информационные модели. Именно здесь проявляется важный инженерный парадокс: протокол, который кажется сложнее на этапе первого знакомства, нередко оказывается удобнее и дешевле на протяжении жизненного цикла системы, потому что лучше поддерживает диагностику, заменяемость и интеграцию [5, 8, 12, 14, 16].

Надежность и живучесть сети. Если говорить о надежности, важно различать как минимум три аспекта. Первый — временная надежность, то есть способность системы стабильно выдерживать требуемый цикл и джиттер. Здесь наиболее сильны EtherCAT и PROFINET IRT, а при корректном проектировании — также EtherNet/IP с механизмами точной синхронизации [6, 9, 11, 15]. Второй аспект — живучесть при отказах линии или узла. Для PROFINET предусмотрены MRP и MRPD [7], а для EtherNet/IP — кольцевые и отказоустойчивые схемы на базе DLR и других механизмов Ethernet-избыточности [8]. Третий аспект — обслуживаемость и киберустойчивость. С этой точки зрения преимущества дают протоколы и экосистемы, где встроены развитые диагностические модели и современные средства защиты. EtherNet/IP здесь усиливается CIP Security [10], а OPC UA изначально строит обмен вокруг аутентификации, контроля целостности и конфиденциальности [14]. Modbus и PROFIBUS могут быть чрезвычайно надежными в физическом смысле и десятилетиями работать на действующих линиях, однако по диагностике и встроенной защите они обычно уступают более новым решениям. Поэтому ответ на вопрос «какой протокол надежнее» зависит от того, что именно понимать под надежностью: стабильный цикл, отказоустойчивую топологию или кибербезопасность [1, 3, 7, 10, 14].

Какой протокол удобнее в эксплуатации. В небольших проектах, где требуется быстро подключить ПЛК к нескольким приборам, безусловным лидером по простоте остается Modbus RTU/TCP. Для него легко найти как документацию, так и совместимые устройства, а ввод в эксплуатацию обычно сводится к настройке адресов, скорости линии и карты регистров. В новых цехах и линиях автоматизации удобство чаще смещается в сторону PROFINET

или EtherNet/IP, потому что здесь инженер получает не только транспорт, но и более глубокую экосистему: описания устройств, сетевую диагностику, стандартизованные профили и понятную интеграцию со средствами разработки контроллеров. EtherCAT наиболее удобен там, где проект с самого начала ориентирован на motion control, многокоординатные приводы и точную синхронизацию. CANopen удобен для компактных встроенных сетей, где не нужны большие объемы трафика. OPC UA, в свою очередь, удобнее всех там, где основная задача — не передать дискреты за сотни микросекунд, а безопасно и структурированно вывести данные ПЛК на уровень SCADA, MES или облачной аналитики. Следовательно, «удобство» всегда привязано к классу задач, а не существует в отрыве от контекста [2, 5, 8, 11, 12, 14].

Итог. Проведенный обзор показывает, что универсального «лучшего» протокола связи для ПЛК не существует. В современных промышленных системах разумнее говорить не о победителе, а о правильном распределении ролей. Там, где требуется максимально быстрый и детерминированный машинный уровень, оправданы EtherCAT или PROFINET IRT; где нужен сбалансированный промышленный Ethernet с развитой диагностикой и большим количеством устройств, сильны PROFINET и EtherNet/IP; где важны простота и низкая стоимость интеграции периферии, сохраняют значение Modbus и CANopen; где необходимо безопасно и содержательно связать ПЛК с программными платформами предприятия, наиболее естественным выбором становится OPC UA. Для действующих производств важна и стратегия миграции: сохранение PROFIBUS и Modbus на нижнем уровне при постепенном добавлении PROFINET, EtherNet/IP или OPC UA наверху часто оказывается более рациональным, чем полная одномоментная замена всей коммуникационной архитектуры. Следовательно, выбор протокола связи для ПЛК должен основываться на типе объекта, требуемом времени цикла, уровне интеграции, политике кибербезопасности и доступных компетенциях персонала. Именно такая архитектурная логика обеспечивает не только высокую скорость, но и долгосрочную надежность системы в целом [1, 14-16].

Список литературы

1. Galloway B., Hancke G.P. Introduction to Industrial Control Networks // IEEE Communications Surveys & Tutorials. 2013. Vol. 15, No. 2. P. 860-880. URL: <http://hdl.handle.net/2263/57869> (дата обращения: 24.03.2026).
2. Modbus Organization. An Introduction to Modbus. URL: <https://www.modbus.org/introduction-to-modbus> (дата обращения: 24.03.2026).
3. Modbus Organization. Specifications and Implementation Guides. URL: <https://www.modbus.org/modbus-specifications> (дата обращения: 24.03.2026).
4. PROFIBUS & PROFINET International. PI Technology PROFIBUS. URL: <https://www.profibus.com/technologies/profibus> (дата обращения: 24.03.2026).
5. PROFIBUS & PROFINET International. PROFINET - Industrial Ethernet Protocol. URL: <https://www.profibus.com/technologies/profinet> (дата обращения: 24.03.2026).

6. PROFIBUS & PROFINET International. PROFIdrive & Encoder. URL: <https://www.profibus.com/technologies/profidrive-encoder> (дата обращения: 24.03.2026).
7. PROFIBUS & PROFINET International. PROFINET Media Redundancy Guideline. URL: <https://www.profibus.com/download/profinet-media-redundancy-guideline> (дата обращения: 24.03.2026).
8. ODVA. EtherNet/IP. URL: <https://www.odva.org/technology-standards/key-technologies/ethernet-ip/> (дата обращения: 24.03.2026).
9. ODVA. CIP Sync. URL: <https://www.odva.org/technology-standards/distinct-cip-services/cip-sync/> (дата обращения: 24.03.2026).
10. ODVA. CIP Security. URL: <https://www.odva.org/technology-standards/distinct-cip-services/cip-security/> (дата обращения: 24.03.2026).
11. EtherCAT Technology Group. EtherCAT - the Ethernet Fieldbus. URL: <https://www.ethercat.org/en/technology.html> (дата обращения: 24.03.2026).
12. CAN in Automation (CiA). CANopen. URL: <https://www.can-cia.org/can-knowledge/canopen> (дата обращения: 24.03.2026).
13. CAN in Automation (CiA). CANopen lower layers. URL: <https://www.can-cia.org/can-knowledge/canopen-lower-layers> (дата обращения: 24.03.2026).
14. OPC Foundation. OPC Unified Architecture; UA Part 1: Security model; OPC UA for Factory Automation. URL: <https://opcfoundation.org/about/opc-technologies/opc-ua/>;
<https://reference.opcfoundation.org/Core/Part1/v105/docs/4.4.1>;
<https://opcfoundation.org/factory/> (дата обращения: 24.03.2026).
15. Wu X., Xie L. Performance evaluation of industrial Ethernet protocols for networked control application // Control Engineering Practice. 2019. Vol. 84. P. 208-217. DOI: 10.1016/j.conengprac.2018.11.022.
16. Tapia E., Sastoque-Pinilla L., Lopez-Novoa U., Bediaga I., Lopez de Lacalle N. Assessing Industrial Communication Protocols to Bridge the Gap between Machine Tools and Software Monitoring // Sensors. 2023. Vol. 23, No. 12. Art. 5694. DOI: 10.3390/s23125694.