CODESYS

Отчет об информационной безопасности

Версия: 9.0
Шаблон: templ_tecdoc_en_V3.0.docx
Имя файла: CODESYS Security Whitepaper.docx
Перевод: oscat.ru

Оглавление

1. Информационная безопасность промышленных систем автоматизации

1.1. Вступление

С развитием информационных технологий процесс передачи данных между компьютерными сетями значительно упростился. Это привело к необходимости проработки вопросов защиты информации и обеспечения безопасности сетевой инфраструктуры. Уже достаточно давно информационная безопасность (ИБ) является неотъемлемой составляющей финансовых систем, корпоративных сетей и т.д. Тем не менее, до недавнего времени не уделялось серьезных мер по обеспечению информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП).

Ситуация кардинально изменилась после инцидента с вирусом Stuxnet. Правительственные организации (такие, как ICS-Cert и BSI) обратили внимание на резкое увеличение числа нарушений информационной безопасности на фабриках, заводах и других промышленных объектах. Консультанты по безопасности начали проводить аудит промышленных систем управления. В наши дни актуальность обеспечения ИБ таких систем не вызывает сомнений и закладывается еще на стадии проектирования объекта. Целью предпринимаемых защитных мер является обеспечение:

- нормального функционирования оборудования, управляющего процессом;
- нормального функционирования прикладного ПО, управляющего процессом;
- конфиденциальности передаваемых данных и исходных кодов прикладного ПО;
- целостности прикладного ПО;
- подлинности оборудования и ПО.

По мере расширения функционала систем управления должны развиваться и требования к их безопасности. Тем не менее, невозможно достичь абсолютной (100%-й) безопасности. Даже если система разработана с применением самых современных средств защиты, она может быть уязвимой за счет уязвимостей в электронных компонентах (процессорах и т.д.), а также в системном и прикладном ПО, которое обычно разрабатывается сторонними организациями.

1.2. Цель документа

Этот документ позволит производителям оборудования, системным интеграторам и операторам обеспечить информационную безопасность своих систем автоматизации, в которых используются устройства, программируемые в среде CODESYS на языках стандарта МЭК 61131-3. Документ описывает общие аспекты ИБ в промышленности, зоны ответственности сторон, участвующих в создании систем автоматизации, и средства CODESYS (существующие и запланированные к разработке), которые позволят обеспечить безопасность создаваемых систем. Кроме того, описывается процесс устранения обнаруженных в CODESYS уязвимостей.

1.3. Выводы

Для обеспечения безопасности системы управления должен быть применен комплекс мер, затрагивающих все потенциальные уязвимости конкретного промышленного объекта, в том числе вероятность некорректного использования системы и угрозы кибератак различной степени тяжести. Невозможно обеспечить достаточный уровень безопасности с помощью всего лишь одного средства защиты.

Следует понимать, что некоторые меры безопасности потребуют дополнительных затрат, например:

- обеспечение контроля физического доступа к критически важным объектам/системам/устройствам;
- обеспечение резервирования питания устройств;
- обучение инженеров-программистов и операторов;
- увеличение времени на разработку прикладного ПО и усложнение эксплуатации из-за введения защитных мер (например, авторизации пользователей в системе).

Каждая компания, которая заказывает системы автоматизации, должна сама определить требуемый баланс между степенью защиты и удобством эксплуатации. Производители оборудования должны предоставлять подходящие средства обеспечения безопасности, которые могут быть использованы системными интеграторами и операторами.

Среда CODESYS содержит ряд таких средств, которые описаны в п. 5. Эти средства ни в коем случае не снимают ответственность с системных интеграторов и операторов, которые должны проводить оценку возможных угроз и предпринимать соответствующие меры. Но, тем не менее, они могут помочь в обеспечении информационной безопасности систем управления.

2. Термины и определения

2.1. Цель атаки

Промышленные системы автоматизации предназначены для управления техническими процессами и производствами. Для нарушения нормального функционирования злоумышленники должны осуществить атаку на один или несколько ключевых компонентов этих систем. Такими компонентами (см. рис. 1) являются:

- контроллер (ПЛК);
- приложение, выполняемое контроллером;
- среда разработки приложений;
- вся система в целом.

2.2. Уязвимости

Ниже представлены примеры уязвимостей системы автоматизации:

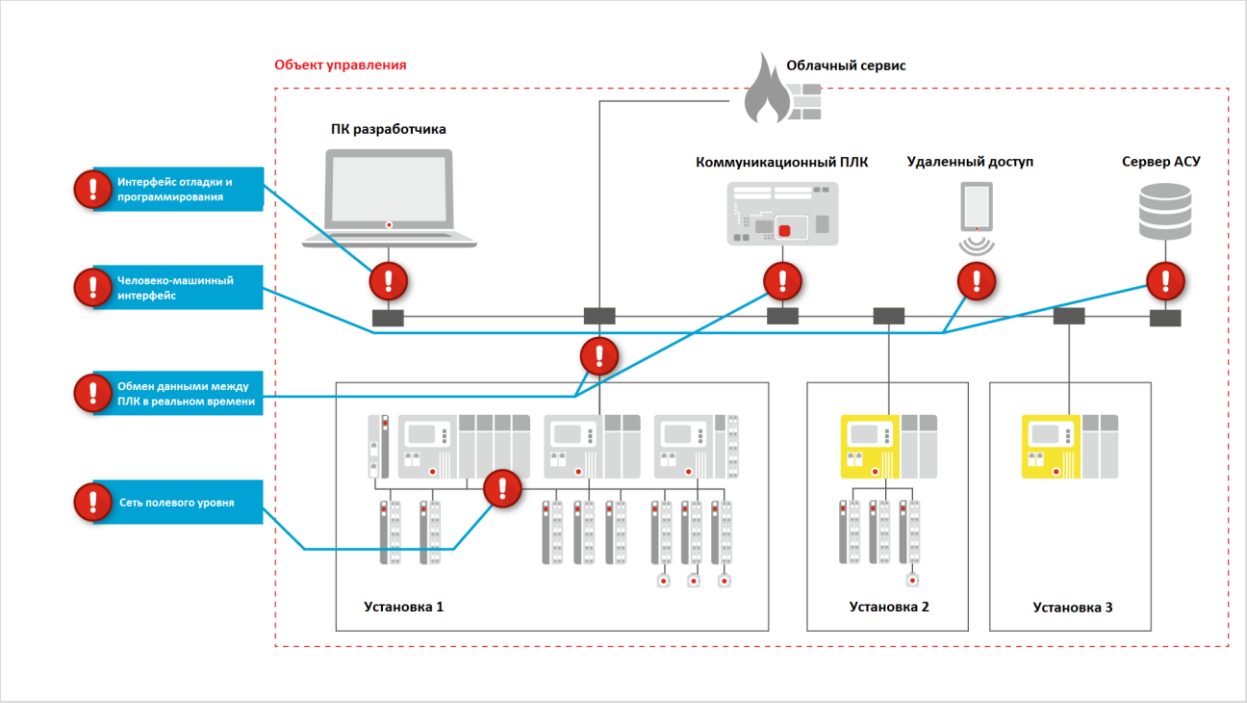

Рис. 1. Примеры уязвимостей системы автоматизации

2.3. Уровни безопасности

Стандарт МЭК 62443 определяет следующие уровни информационной безопасности:

- **Уровень 1**: предотвращение неавторизованного раскрытия информации посредством ее несанкционированного извлечения или случайного обнародования.
  Примеры угроз: ошибка оператора, неисправность ПК

- **Уровень 2**: предотвращение неавторизованного раскрытия информации субъекту, активно ее ищущему с использованием простых средств, при незначительных ресурсах, посредственных навыках и низкой мотивации.
  Примеры угроз: подбор пароля

- **Уровень 3**: предотвращение неавторизованного раскрытия информации субъекту, активно ее ищущему с использованием изощренных средств при умеренных ресурсах, наличии специальных познаний в области АСУ ТП и умеренной мотивации.
  Примеры угроз: использование готового ПО для взлома

- **Уровень 4**: предотвращение неавторизованного раскрытия информации субъекту, активно ее ищущему с использованием изощренных средств при обширных ресурсах, наличии специальных познаний в области АСУ ТП и высокой мотивации.
  Примеры угроз: разработка специального ПО для взлома с учетом наличия информации о внутреннем устройстве системы

2.4. Контроллер

Контроллер – это промышленный компьютер, применяемый для автоматизации технологических процессов и производств. Для его обозначения могут быть использоваться термины ПЛК[1] (PLC), ПКА[2] (PAC), контроллер управления движением (Motion Controller), блок управления (ECU[3]), РСУ[4] (DCS), система управления процессами (PCS[5]) и т.д. В данном документе под терминами «контроллер» и «ПЛК» подразумеваются все перечисленные типы устройств. Независимо от используемого для его обозначения термина, контроллер обычно является центром системы управления и поэтому представляет собой основную цель для атак. Кроме того, контроллер является программируемым устройством, и полный запрет на его перепрограммирование после установки на объекте фактически невозможен, так как приложение с высокой вероятностью будет дорабатываться в процессе эксплуатации. Интерфейс программирования является потенциально опасной точкой воздействия, для использования которой могут быть не нужны специальные навыки. Поэтому обеспечение информационной безопасности контроллеров должно являться одной из приоритетных задач системных интеграторов и операторов.

[1] Программируемый логический контроллер (Programmable Logic Controller)
[2] Программируемый контроллер автоматизации (Programmable Automation Controller)
[3] Electronic Control Unit
[4] Распределенная система управления (Distributed Control System)
[5] Process Control System

2.5. Приложение

Приложение – это совокупность программных компонентов, необходимых для выполнения контроллером требуемой задачи. Приложение загружается в контроллер через интерфейс программирования.

2.6. Угроза

Нормальное функционирование системы управления может быть нарушено различными способами. Основные меры безопасности предназначены для защиты от преднамеренных атак, таких как саботаж и шпионаж. Тем не менее, угрозами можно также считать самопроизвольный выход из строя аппаратного/программного обеспечения и непреднамеренные ошибки, совершенные из-за человеческого фактора (например, ввод оператором некорректных значений уставок).

2.7. Система безопасности

Все системы управления техническими процессами должны быть оснащены системой безопасности, которая предназначена для предотвращения умышленного или случайного нарушения нормального функционирования объекта управления. Следует помнить, что система управления не может быть полностью изолированной, так как требует доступа во время установки, наладки и сервисного обслуживания. Поэтому требуется разделить систему управления на подсистемы и обеспечить для каждой из таких подсистем контроль доступа. Более подробная информация по этому вопросу приведена в п. 3.1.

3. Общие средства защиты промышленных систем управления

В промышленных системах управления должны использоваться те же меры безопасности, что и в обычных компьютерных сетях:

- антивирусное ПО;
- использование паролей высокого уровня надежности и их регулярное изменение;
- межсетевые экраны (Firewall);
- VPN-туннели для связи удаленных сетей;
- контроль использования носителей информации (например, USB Flash).

Также требуется обеспечить аутентификацию пользователей для доступа к контроллерам и сетям объекта.

Кроме того, для промышленных объектов требуется ряд дополнительных специфических мер безопасности, описанных ниже.

3.1. Ограничение доступа

Доступ к контроллерам (как физический, так и сетевой) должен быть ограничен. Примерами таких ограничений могут являться:

- размещение контроллеров в запираемых на ключ шкафах управления;
- использование на объекте сетей, изолированных от Интернета, или же сетей с доступом из Интернета, но только через VPN-туннель с тщательно настроенным межсетевым экраном.

При создании сетей на промышленном объекте следует придерживаться следующих правил:

- сети, связывающие контроллеры и другие устройства автоматизации, должны быть изолированы от других сетей и не включать себя устройств, не требуемых для процесса управления;
- обмен между контроллерами и устройствами полевого уровня, осуществляемый через стандартные промышленные протоколы (fieldbus), должен быть защищен стандартными мерами безопасности (см. выше). Промышленные протоколы обычно не имеют встроенных средств безопасности (например, шифрования), поэтому физический или программный доступ к таким сетям является серьезной угрозой безопасности.

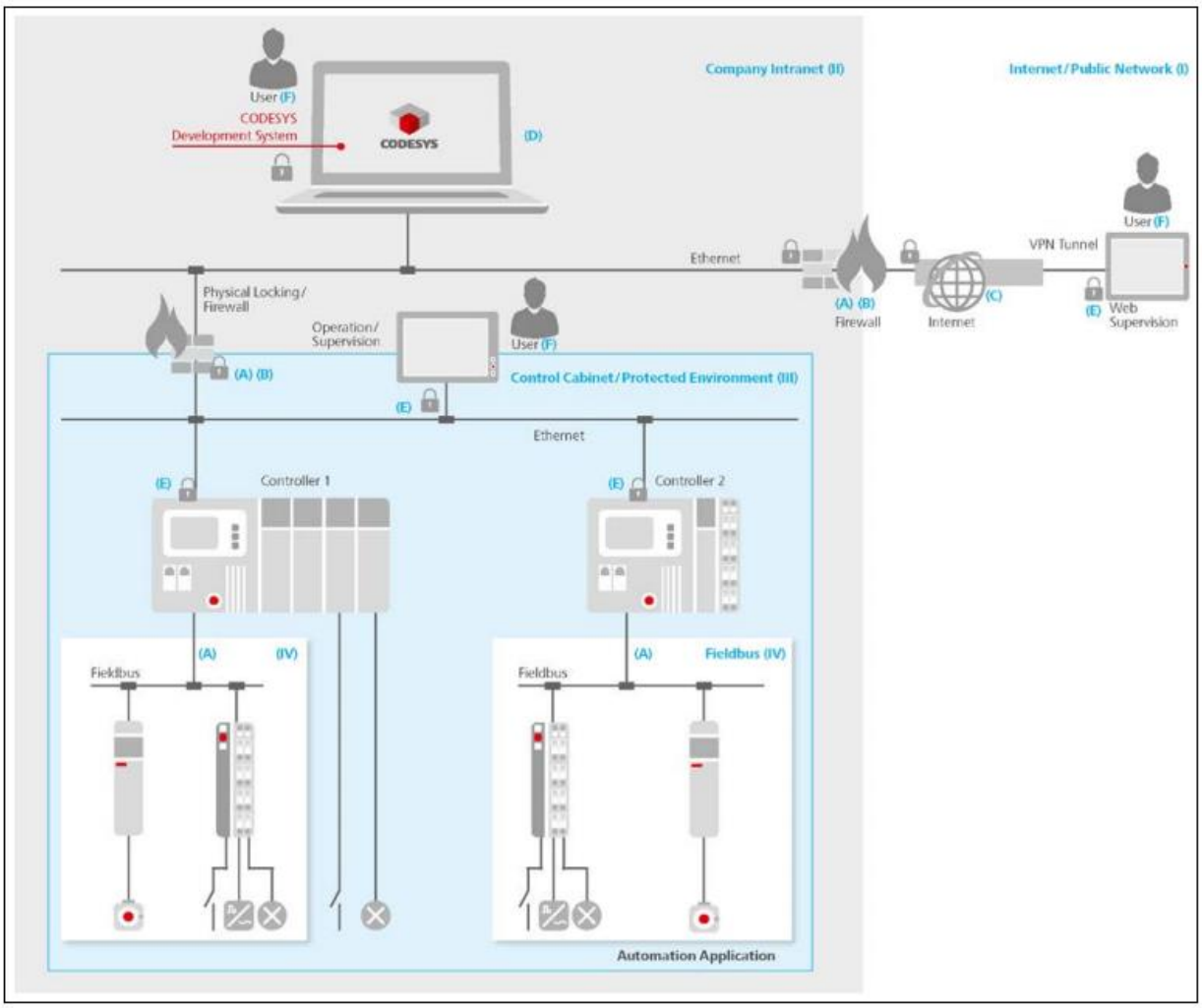

Рис. 2. Типовая структура сетей промышленного объекта

На рисунке 2 цифрами выделены различные сети (полностью изолированные или защищенные межсетевым экраном):

- I – внешняя сеть (например, Интернет);
- II – сеть предприятия;
- III – сеть системы управления;
- IV – сеть устройств полевого уровня (fieldbus).

Буквами обозначены различные средства безопасности:

- A – физическое ограничение доступа;
- B – межсетевой экран[6] (Firewall);
- C – VPN;
- D – антивирусное ПО, ограничение прав пользователей ПК;
- E – аутентификация пользователей (пароли, USB-ключи);
- F – проведение обучения по информационной безопасности.

[6] Межсетевой экран между сетями II и III должен обеспечивать защиту в обоих направлениях.

3.2. Обучение персонала

Большинство известных инцидентов с нарушением безопасности промышленных объектов было связано не с преднамеренной атакой, а с ошибками оператора или оборудования. Таким образом, ключевую роль в обеспечении безопасности АСУ ТП играют производители оборудования и пользователи систем управления. Они должны быть информированы о возможных угрозах информационной безопасности и средствах их предотвращения.

Пользователи CODESYS также должны знать о доступных в среде мерах безопасности, которые могут быть использованы при разработке приложения контроллера. Для этого рекомендуется провести специальное обучение для программистов (внутреннее в рамках компании или с привлечением внешних специалистов).

4. Кто ответственен за безопасность АСУ?

В процессе создания и эксплуатации систем автоматизации участвуют несколько сторон: поставщики оборудования и ПО, системные интеграторы, операторы. Поскольку обеспечение информационной безопасности является комплексной задачей, то каждая из сторон должна приложить определенные усилия в этом направлении.

Рис. 3. Отношения различных сторон при обеспечении безопасности АСУ

Более подробная информация о ролях и ответственности сторон приведена в стандарте VDI/VDE2182.

5. Средства безопасности в CODESYS

Одной из целей разработчиков CODESYS является предоставление пользователю средств защиты своего контроллера и приложения. Эти средства направлены на обеспечение уровней безопасности 1 и 2 (см. п. 2.3). В перспективе планируется разработка средств защиты для уровня 3.

CODESYS состоит из двух платформ: интегрированной среды разработки (CODESYS Development System, также называемой CODESYS IDE), которая устанавливается на ПК программиста, и системы исполнения (CODESYS Control), которая устанавливается в контроллер его производителем. Среда разработки и система исполнения всегда используются совместно, поэтому средства безопасности затрагивают обе платформы. Кроме того, CODESYS предоставляет программисту средства защиты, которые активируются из кода приложения контроллера. CODESYS позволяет создавать различные виды визуализации, которая дает возможность непосредственно влиять на технологический процесс и поэтому также содержит встроенные средства защиты.

В следующих разделах описываются средства безопасности, которые доступны (или будут доступны) в последних на данный момент версиях CODESYS. Одним из методов обеспечения безопасности является использование самой свежей версии среды разработки и системы исполнения. Обнаруженные уязвимости исправляются с помощью патчей (см. п. 7), поэтому использование актуальных версий ПО позволяет уменьшить число уязвимостей, а также применять наибольшее количество средств защиты.

В таблице ниже приведен обзор средств защиты, доступных в CODESYS. Для каждого средства описан тип угроз, против которых оно направлено, и перечислены категории лиц, участвующих в создании системы управления, которые должны способствовать его внедрению. Более подробная техническая информация о каждом средстве защиты доступна в CODESYS Online Help.

CODESYS Development System (среда программирования)

Средство защиты	Описано в пункте	Кем внедряется			Защищает от
		Производители оборудования	Системные интеграторы	Операторы	
Шифрование исходного кода проекта	5.1.1		+		случайных и непредумышленных угроз
Управление пользователями проекта	5.1.2		+		случайных и непредумышленных угроз
Подпись скомпилированных МЭК-библиотек	5.1.3	+	+	+	предумышленных угроз
Подпись пакетов CODESYS	5.1.4	+	+	+	предумышленных угроз

CODESYS Runtime System (система исполнения)

Средство защиты	Описано в пункте	Категория пользователей			Защищает от
		Производители оборудования	Системные интеграторы	Операторы	
Ограничение доступа к системе исполнения с использованием аутентификации и разграничения прав пользователей	5.2.1	+	+	+	случайных и непредумышленных угроз
Шифрование и подпись загрузочного приложения	5.2.2	+	+		предумышленных угроз
Выбор режима работы ПЛК	5.2.3		+		случайных и непредумышленных угроз
Подтверждение подключения к ПЛК из CODESYS IDE	5.2.4	+	+		случайных и непредумышленных угроз
Резервное копирование и восстановление файлов ПЛК, относящихся к приложению CODESYS	5.2.5	+	+	+	случайных и непредумышленных угроз
Шифрование соединения между ПЛК и CODESYS IDE	5.2.6	+	+	+	предумышленных угроз
Средства безопасности сервера OPC UA	5.2.7	+	+	+	нарушения целостности и/или конфиденциальности информации
Ограничение доступа к символьной конфигурации	5.2.8	+	+	+	нарушения конфиденциальности информации
Запись журнала аудиторского следа	5.2.9			+	случайных и непредумышленных угроз

Приложение

Средство защиты	Описано в пункте	Категория пользователей			Защищает от
		Производители оборудования	Системные интеграторы	Операторы	
Ограничение функционала, доступного при подключении к ПЛК	5.3.1	+	+		случайных и непредумышленных угроз
Защита приложения с помощью аппаратного ключа	5.3.2	+	+		случайных и непредумышленных угроз

Визуализация

Средство защиты	Описано в пункте	Категория пользователей			Защищает от
		Производители оборудования	Системные интеграторы	Операторы	
Управление пользователями визуализации	5.4.1		+	+	случайных и непредумышленных угроз
Шифрование трафика web-визуализации	5.4.2	+	+	+	предумышленных угроз

5.1. Средства безопасности в среде программирования

5.1.1. Шифрование исходного кода проекта

Средство защиты для системных интеграторов

Исходный программный код приложения контроллера содержит информацию о функционировании объекта управления и является интеллектуальной собственностью его создателя. Поэтому защита исходного кода имеет высокий приоритет, особенно если он содержит конфиденциальные сведения.

В среде программирования CODESYS доступ к исходному коду проекта может быть защищен паролем или аппаратным ключом (CODESYS Key). При использовании пароля применяется алгоритм шифрования AES, при использовании аппаратных ключей – проприетарное ПО от компании WIBU Systems. Без наличия пароля или аппаратного ключа зашифрованный проект не может быть открыт и отредактирован.

Преимуществом использования пароля является простота и отсутствие необходимости в приобретении аппаратных ключей. С другой стороны, защита проекта аппаратным ключом является более надежной, так как вероятность утечки пароля значительно выше. Кроме того, каждый проект можно связать с несколькими аппаратными ключами, обеспечив таким образом контролируемый доступ нужной группе сотрудников. Риск потери доступа к исходному коду проекта из-за утраты аппаратного ключа можно снизить, изготовив одну или несколько его резервных копий.

Начиная с версии CODESYS V3.5 SP10 исходный код проекта может быть защищен сертификатом X.509. В этом случае для защиты проекта используется симметричный алгоритм шифрования (AES). Симметричный ключ шифруется ассиметричным алгоритмом (RSA) с помощью открытого ключа пользователя, работающего с проектом. При необходимости проект также может быть помечен цифровой подписью с использованием закрытого ключа, связанного с сертификатом X.509 текущего пользователя. Подпись будет сохранена вместе с проектом в виде файла с расширением .p7s в формате, определенном стандартом PKCS#7.

При открытии подписанного проекта его содержимое сопоставляется с подписью. Если подпись недействительна, пользователь увидит предупреждающее сообщение и сможет сделать осознанный выбор: открыть проект или отменить эту операцию.

Описанное средство предназначено для защиты интеллектуальной собственности.

5.1.1.1. Проверка целостности проекта

Если шифрование не используется, то файл проекта сохраняется в проприетарном формате CODESYS, и при каждом его открытии выполняется проверка целостности. Эта проверка доступна и включена по умолчанию, начиная с версии CODESYS V3.5 SP13. Данный функционал несовместим с более ранними версиями среды программирования. Для повышения уровня защиты проекта рекомендуется использовать одно из средств, упомянутых п. 5.1.1.

Описанное средство используется для проверки целостности файла проекта и детектирования его повреждения.

5.1.2. Управление пользователями проекта

Средство защиты для системных интеграторов

В дополнение к защите всего исходного кода проекта CODESYS предоставляет возможность защитить отдельные объекты проекта от чтения/записи с помощью механизма управления пользователями. Такая защита может быть установлена на команды меню, а также на создание конкретных типов объектов (например, на задач, POU, методов, списков глобальных переменных и т. д.) или редактирование существующих объектов (например, задач, POU или узла настроек проекта).

Кроме того, с помощью управления пользователями можно точечно ограничить доступный функционал проекта. Права доступа могут быть адаптированы к конкретным требованиями безопасности (например, критически важные с точки зрения безопасности функции – такие, как скрипты – могут быть настроены только для применения пользователями, которые имеют явные разрешения на такие действия).

Описанное средство используется для защиты интеллектуальной собственности и обеспечения целостности файла проекта.

5.1.3. Подпись скомпилированных МЭК-библиотек

Средство защиты для производителей оборудования, системных интеграторов и операторов

CODESYS поддерживает подпись МЭК-библиотек сертификатом X.509, если они сохраняются в скомпилированном виде (.compiled-library). Хотя сам факт компиляции библиотеки обеспечивает защиту ее исходного кода, подпись позволяет проверить целостность и подлинность. Подписанные библиотеки отмечаются в менеджере библиотек проекта CODESYS специальной иконкой. Часто в состав библиотеки входят файлы документации или дополнительные файлы, используемые в визуализации. Действие подписи распространяется не только на исходный код библиотеки, но и на эти вложенные файлы. Документы или файлы, вложенные в библиотеку, доступны для отображения (или исполнения) только в том случае, если библиотека была корректно подписана действительным сертификатом. По этой причине все недавно выпущенные или обновленные библиотеки от разработчиков CODESYS подписаны, что позволяет определить их подлинность и надежность. CODESYS GmbH призывает всех разработчиков библиотек подписывать их, чтобы пользователи могли подтвердить их подлинность.

Описанное средство доказывает подлинность и целостность скомпилированных библиотек CODESYS и предотвращает непреднамеренное использование ненадежных библиотек.

5.1.4. Подпись пакетов CODESYS

Средство защиты для производителей оборудования, системных интеграторов и операторов

CODESYS поддерживает подпись пакетов сертификатом X.509. Пакеты CODESYS содержат дополнительные функции или плагины. Установка пакетов выполняется с помощью менеджера пакетов среды разработки CODESYS.

Менеджер пакетов проверяет, имеет ли устанавливаемый пакет корректную подпись, основанную на действующем сертификате. Поэтому все пакеты, выпускаемые разработчиками CODESYS, подписываются.

CODESYS GmbH призывает всех разработчиков пакетов подписывать их, чтобы пользователи могли подтвердить их подлинность.

Описанное средство доказывает подлинность и целостность пакетов CODESYS и предотвращает непреднамеренное использование ненадежных пакетов.

5.2. Средства безопасности в системе исполнения CODESYS

5.2.1. Ограничение доступа к системе исполнения с использованием аутентификации и разграничения прав пользователей

Средство защиты для производителей оборудования, системных интеграторов и операторов

Создание автоматизированной системы управления состоит из нескольких этапов – начиная от разработки приложения для контроллера и заканчивая вводом в эксплуатацию с последующим сервисным обслуживанием. На каждом из этапов с системой работают инженеры различного уровня квалификации.

Присутствие персонала с различным уровнем квалификации и угроза их воздействия на систему в собственных интересах приводит к необходимости ограничения доступа к оборудованию. CODESYS включает в себя механизм аутентификации пользователей и распределения их по группам с заданными полномочиями.

По умолчанию в системе исполнения CODESYS Control включен механизм онлайн-управления пользователями, которое должен быть активировано, прежде чем клиенты смогут подключаться к системе исполнения. Такими клиентами являются:

- среда разработки CODESYS;
- система визуализации CODESYS HMI;
- приложения, использующие PLC Handler;
- CODESYS OPC DA Server;
- клиенты, подключающиеся по протоколу OPC UA.

Активировать управление пользователями можно путем подключения к контроллеру из среды разработки CODESYS. Во время первого подключения пользователь должен создать пользователя-администратора и задать для него логин и пароль.

С помощью соответствующих команд среды разработки CODESYS администратор может создавать в среде разработки группы пользователей, ограничивать доступный им функционал, создавать и удалять пользователей, распределять их по группам. Редактор пользователей является простым и в то же время гибким.

Мы рекомендуем использовать учетную запись администратора только для целей менеджмента – например, для создания новых пользователей или настройки онлайн-управления пользователями. Для оперативного доступа к системе исполнения CODESYS Control необходимо создать отдельных пользователей и добавить их в группу, для которой назначены лишь те права, которые необходимы для выполнения их профессиональных обязанностей.

Чтобы гарантировать, что ни один злоумышленник не сможет взломать контроллер сразу после ввода в эксплуатацию – первый запуск системы исполнения CODESYS Control должен осуществляться исключительно в безопасной среде. В этой среде должны быть произведены все этапы инсталляции: от установки системы исполнения CODESYS Control до активации управления пользователями путем создания первого пользователя-администратора.

После создания пользователей каждое подключение к контроллеру из среды разработки будет сопровождаться появлением окна аутентификации, в котором нужно будет ввести логин и пароль. Пароли передаются в зашифрованном виде (по умолчанию с использованием асимметричной криптографии) и сохраняются в системе исполнения в виде хэшей.

В соответствии с уровнями безопасности 1 и 2 это позволяет защитить контроллер от случайного или умышленного доступа и обеспечить целостность приложения.

5.2.2. Шифрование и подпись загрузочного приложения

Средство защиты для производителей оборудования и системных интеграторов

Разработка приложения ПЛК завершается с вводом системы в эксплуатацию (с учетом возможности внесения доработок во время сервисного обслуживания). Приложение загружается в контроллер в скомпилированном виде, и, следовательно, не содержит исходных кодов. Тем не менее, при получении доступа к скомпилированному приложению существует возможность дизассемблирования – например, в целях воспроизведения системы. Очевидно, что это является нарушением интеллектуальной собственностью разработчиков. Поэтому разумно произвести шифрование загрузочного приложения.

5.2.2.1. Шифрование с помощью CodeMeter®

Одним из вариантов шифрования является использование аппаратного ключа с поддержкой технологии CodeMeter® от компании WIBU Systems. Таким ключом может являться специальный USB-накопитель (CODESYS Key) или карта памяти, поставляемая WIBU Systems. Первый

вариант подходит для ПЛК с ОС Windows или Linux, второй – для устройств со специфичной ОС (или вообще без ОС) и устройств, не имеющих интерфейса USB. Каждый аппаратный ключ имеет уникальный серийный номер. Во время загрузки проекта в ПЛК его приложение шифруется с использованием этого номера.

После шифрования приложение будет выполняться только на контроллере с подключенным аппаратным ключом. Кроме того, дизассемблирование приложения не даст доступа к его исходным кодам. Это позволяет защитить интеллектуальную собственность и избежать нелегального воспроизведения системы управления.

5.2.2.2. Шифрование и подпись приложения с использованием сертификатов X.509

Начиная с версии CODESYS V3.5 SP10 загрузочное приложение может быть зашифровано и защищено сертификатом(-ми) X.509. Это является альтернативой использованию технологии CodeMeter®. Приложение будет выполняться только на том контроллере, который содержит закрытый ключ связанного с приложением сертификата. Можно связать приложение сразу с несколькими сертификатами, чтобы обеспечить его выполнение на разных контроллерах.

Это позволяет защитить интеллектуальную собственность и предотвратить выполнение приложений, загруженных неидентифицированными пользователями.

Управление сертификатами X.509 в среде разработки CODESYS осуществляется с помощью плагина CODESYS Security Agent. Подробная информация о работе с ним приведена в документации.

5.2.3. Выбор режима работы контроллера

Средство защиты для системных интеграторов

На этапе отладки системы управления допускается регулярная загрузка обновленного приложения в контроллер. Но после ввода системы в эксплуатацию такая ситуация уже является неприемлемой.

Чтобы избежать подобных случаев CODESYS позволяет установить режим работы контроллера. В режиме «Отладка», который включен по умолчанию, допускается выполнение любых команд, в том числе удаление и обновление приложения. В режиме «Заблокировано» у программиста нет возможности загрузки приложения – это может быть полезно, если в сети присутствует несколько ПЛК, но в отладке находится только несколько из них. «Рабочий» режим используется после ввода контроллера в эксплуатацию. В этом режиме запрещены любые команды, влияющие на приложение (загрузка, удаление и т.д.).

Возможность переключения режимов может быть доступна только для заданных пользователей с помощью средств из п. 5.2.1.

Описанное средство используется для предотвращения непредумышленного доступа к контроллеру и сохранения целостности приложения.

5.2.4. Подтверждение подключения к контроллеру из CODESYS IDE

Средство защиты для производителей оборудования и системных интеграторов

Если в сети находится несколько контроллеров, то программист случайно может подключиться не к тому, к которому предполагал. В некоторых ситуациях это может представлять угрозу безопасности. Для предотвращения подобных проблем в CODESYS присутствует режим интерактивного логина. В этом режиме подключение к контроллеру должно быть явно подтверждено с помощью ввода его серийного номера или нажатием кнопки на корпусе. Альтернативным вариантом является детектирование контроллером подключения пользователя – например, с помощью мигания светодиода или звукового сигнала.

Описанное средство используется для предотвращения непредумышленного доступа к контроллеру и сохранения целостности приложения.

5.2.5. Резервное копирование и восстановление файлов ПЛК, относящихся к приложению CODESYS

Средство защиты для производителей оборудования, системных интеграторов и операторов

Защита от непредумышленного доступа снижает вероятность нарушения целостности приложения, но не исключает такой возможности – например, в случае выхода контроллера из строя. Для уменьшения времени простоя оборудования в этой ситуации в CODESYS предусмотрена возможность резервного копирования и восстановления проекта.

5.2.6. Шифрование соединения между контроллером и CODESYS IDE

Средство защиты для производителей оборудования, системных интеграторов и операторов

Даже если доступ к контроллеру требует аутентификации, канал связи между ПЛК и средой программирования может быть взломан с целью перехвата паролей и других передаваемых данных. Для предотвращения этой угрозы весь передаваемый трафик между контроллером и CODESYS IDE может быть зашифрован с использованием протокола TLS 1.2.

Описанное средство используется для предотвращения предумышленного доступа к контроллеру.

Возможно ли шифрование соединения или нет – зависит от политики безопасности системы исполнения. Можно выбрать одну из следующих политики безопасности:

- Без шифрования – шифрование соединения невозможно;
- Опциональное шифрование – возможно как зашифрованное соединение, так и незашифрованное;
- Принудительное шифрование – возможно только зашифрованное соединение.

См. также информацию о работе с сертификатами X.509 в среде CODESYS в п. 5.2.2.2.

5.2.7. Средства безопасности сервера OPC UA

Средство защиты для производителей оборудования, системных интеграторов и операторов

OPC UA – это промышленный протокол обмена, разработанный организацией OPC Foundation. Система исполнения CODESYS может включать в себя сервер OPC UA. Ниже перечислены средства безопасности, которые рекомендуется применять в случае использования данного протокола.

5.2.7.1. Сервер OPC UA: использование сертификата X.509

Протокол OPC UA поддерживает использование сертификатов X.509. Профили безопасности разработаны организацией OPC Foundation. Данное средство позволяет обеспечить целостность (для профилей с подписью) или целостность и конфиденциальность (для профилей с подписью и шифрованием) передаваемых данных.

Данный функционал поддерживается с версии CODESYS V3.5 SP11.

См. также информацию о работе с сертификатами X.509 в среде CODESYS в п. 5.2.2.2.

5.2.7.2. Сервер OPC UA: управление пользователями

Управление пользователями позволяет ограничить подключение к серверу OPC UA для неавторизованных лиц. Это позволяет обеспечить конфиденциальность передаваемых данных.

Данный функционал поддерживается с версии CODESYS V3.5 SP13.

5.2.8. Ограничение доступа к символьной конфигурации

Средство защиты для производителей оборудования, системных интеграторов и операторов

Символьная конфигурация – это механизм CODESYS, который позволяет обеспечить обмен данными между контроллером и другими устройствами или ПО (в частности, символьная конфигурация используется для работы с CODESYS OPC DA Server).

В символьной конфигурации можно создавать группы символов, для каждой из которых можно настроить пользователей и их права (только чтение или чтение/запись). Это позволяет обеспечить конфиденциальность передаваемых данных.

Данный функционал поддерживается с версии CODESYS V3.5 SP13.

5.2.9. Запись журнала аудиторского следа

Средство защиты для операторов

Система исполнения CODESYS Control включает в себя развитые средства логирования. В дополнение к системному журналу, который в основном содержит информацию о системе и ее конфигурации, а также сообщения об ошибках, журнал аудиторского следа содержит сообщения, которые могут использоваться при анализе инцидентов, связанных с информационной безопасностью.

В журнале аудиторского следа сохраняется как информация о действии пользователей, так и системные события. Например:

- Управление пользователями
  - информация о неуспешных попытках входа;
  - вход в систему;
  - выход из системы;
  - изменение конфигурации пользователей (добавление пользователей, удаление пользователей, изменение прав, изменение паролей и т. д.)
- Приложение CODESYS
  - запуск / остановка / сброс;
  - установка точек останова;
  - форсирование (принудительная запись) значений переменных;
  - загрузка приложения или его онлайн-обновление.
- Системные события
  - загрузка системы исполнения;
  - запуск пользовательского приложения.

Все бэкэнды, доступные для системного журнала, могут использоваться и для журнала аудиторского следа. Зарегистрированные события можно отображать непосредственно в среде разработке CODESYS при подключении к контроллеру, отправлять на syslog-сервер и сохранять в файлы. Для последнего варианта можно настроить ограничение на количество записей в файле и размер файла. В зависимости от настроек, файлы журналов создаются непрерывно (после заполнения очередного файла – создается следующий) или перезаписываются в режиме кольцевого буфера (новые файлы перезаписывают самые старые) – это эффективно предотвращает заполнение файловой системы.

Описанное средство используется для отслеживания случайных, непредумышленных и предумышленных изменений и событий.

5.3. Средства безопасности для приложения

5.3.1. Ограничение функционала, доступного в CODESYS IDE при подключении к контроллеру

Средство защиты для производителей оборудования и системных интеграторов

Разработчик приложения может ограничить доступ к контроллеру из кода программы. Для этого применяется функциональный блок PlcOperationControl из библиотеки *Component Manager*. Он позволяет отключить возможность загрузки приложения в контроллер, остановку приложения, выгрузку файлов и т.д.

Описанное средство используется для предотвращения непредумышленного доступа к контроллеру и обеспечения целостности проекта.

5.3.2. Защита приложения с помощью аппаратного ключа

Средство защиты для производителей оборудования и системных интеграторов

В некоторых случаях приложение включает в себя специальные функции, которые должны использоваться только при наладке системы управления и сервисном обслуживании. Для предотвращения доступа к этим функциям в процессе эксплуатации их можно связать с аппаратным USB-ключом (CODESYS Key). Таким образом, данный функционал будет доступен только авторизованному персоналу. Привязка функций к ключу осуществляется в коде приложения.

Описанное средство используется для обеспечения уровней безопасности 1 и 2.

5.4. Средства безопасности для визуализации

5.4.1. Управление пользователями визуализации

Средство защиты для системных интеграторов и операторов

Визуализация CODESYS позволяет управлять контроллером и, соответственно, всем технологическим процессом. Поэтому настоятельно рекомендуется разделить доступный через визуализацию функционал на отдельные сегменты (например: мониторинг, настройка, управление и т.д.), доступ к которым будет только у пользователей с соответствующими правами. CODESYS включает в себя встроенный механизм управления пользователями, который позволяет ограничить доступ как к экранам визуализации, так и к их отдельным элементам. Для подтверждения доступа будет требоваться аутентификация пользователя. Таким образом, выполнение критических операций (например, запуск и остановка производственной линии) может быть выполнена только ответственным персоналом.

Описанное средство используется для защиты от непредумышленного и предумышленного доступа.

5.4.2. Шифрование трафика web-визуализации

Средство защиты для производителей оборудования, системных интеграторов и операторов

Система исполнения CODESYS может включать в себя web-сервер визуализации. Для предотвращения взлома канала связи между контроллером и web-клиентом (обычно – web-браузером) соединение может быть зашифровано с помощью протокола HTTPS. Это позволяет обеспечить конфиденциальность и целостность данных. Более подробная информация приведена в онлайн-справке CODESYS и документе *WebServerSSL_en.pdf*[7].

См. также информацию о работе с сертификатами X.509 в среде CODESYS в п. 5.2.2.2.

[7] Документ входит в дистрибутив CODESYS. После установки он может быть найден по пути *<папка_установки_CODESYS>\GatewayPLC\Documentation\WebServerSSL_en.pdf*

6. Средства безопасности в CODESYS, запланированные к разработке

Помимо уже существующих средств безопасности запланирована разработка новых. Они описаны в таблице ниже.

Средство защиты	Описано в пункте	Кем внедряется			Защищает от
		Производители оборудования	Системные интеграторы	Операторы	
Упрощение процесса аутентификации	6.1.1		+	+	случайных и непредумышленных угроз
Ограничение доступа по IP-адресу	6.1.2		+		случайных и непредумышленных угроз
Разработка документации и обучающих курсов	6.1.3	+	+	+	случайных и непредумышленных угроз
Режим «только для чтения»	6.1.4		+		случайных и непредумышленных угроз

6.1. Будущие средства безопасности

6.1.1. Упрощение процесса аутентификации

Средство защиты для системных интеграторов и операторов

Одним из средств защиты является аутентификация пользователей (например, с помощью ввода логина и пароля при подключении к контроллеру). Такой способ затрудняет эксплуатацию системы – операторам и техникам придется запоминать свои логины/пароли и тратить дополнительное время на авторизацию. Это приведет к тому, что данные средства защиты могут быть проигнорированы. Решением проблемы является облегчение процесса аутентификации – например, с помощью использования аппаратных ключей (CODESYS Key) или ограничение доступа к сетевым ресурсам (в т.ч. ПЛК) с использованием протокола LDAP.

6.1.2. Ограничение доступа по IP-адресу

Средство защиты для системных интеграторов

В данный момент CODESYS не проверяет IP-адреса пользователей, которые подключаются к контроллеру через интерфейсы программирования и визуализации. Эту проблему поможет решить создание профилей пользователей, которые будут содержать список разрешенных IP-адресов и права доступа для каждого из них (например, только мониторинг без возможности загрузки приложения). Также в профиле можно будет отключить маршрутизацию трафика.

Описанное средство позволит предотвратить непредумышленный доступ к контроллерам, находящимся в публичной сети.

6.1.3. Разработка документации и обучающих курсов

Средство защиты для производителей оборудования, системных интеграторов и операторов

Все описанные в документе средства защиты требуют определенного опыта для настройки и использования. В связи с этим запланирован ряд задач:

- разработка отдельного компонента CODESYS, позволяющего легко настроить все доступные средства защиты (Security Wizard);
- создание дополнительной документации по средствам защиты, в том числе руководства по применению и чек-листа для проверки степени безопасности системы;
- разработка учебного курса по информационной безопасности. В нем будут рассматриваться как универсальные средства защиты (VPN, Firewall), так и специфичные для CODESYS;
- проведение обучения и сертификации специалистов по теме информационной безопасности.

6.1.4. Режим «только для чтения»

Средство защиты для системных интеграторов

При сохранении проектов будет доступа специальная опция, позволяющая запретить внесение в проект каких-либо изменений (это касается как исходных кодов, так и загрузочного приложения для данного проекта). Это позволит обеспечить целостность проекта и приложения.

7. Сетевые порты, используемые CODESYS

Для программирования и обмена данными среда CODESYS использует определенные сетевые порты контроллера. Они перечислены в таблице ниже.

Номер порта	Протокол	Цель использования	Возможность переназначения
1740–1743	UDP / протокол CODESYS	Программирование и клиентский доступ к системе исполнения CODESYS Control	Нет
11740	TCP / протокол CODESYS		Да
1217	TCP / протокол CODESYS Gateway	Обмен данными между клиентом CODESYS Gateway и службой CODESYS Gateway. Большинство клиентов (например, среда разработки) используют CODESYS Gateway как шлюз для подключения к системе исполнения CODESYS Control	Да
8080	TCP / HTTP	Веб-сервер визуализации системы исполнения CODESYS Control	Да
443	TCP / HTTPS	Веб-сервер визуализации системы исполнения CODESYS Control (для подключения с использованием криптографического протокола TLS)	Да
4840	TCP / OPC UA	CODESYS OPC UA Server	Да (с версии CODESYS V3.5 SP7)
443	TCP / WebSocket	Интерфейс облачного сервиса CODESYS Automation Server для подключения с помощью утилиты CODESYS Edge Gateway	Нет
22350	TCP + UDP	Межпроцессный (localhost) обмен между продуктами CODESYS (например, системой исполнения CODESYS Control) и системой исполнения службы контроля лицензий WIBU CodeMeter, запущенной на том же устройстве	Нет

В дополнение к перечисленным портам производители оборудования и системные интеграторы могут использовать другие порты (например, для работы с FTP-сервером, SSH-терминалом и т.д.). Системные интеграторы и операторы несут ответственность за предотвращение несанкционированного доступа к контроллеру через эти порты.

8. Процесс устранения уязвимостей в CODESYS

При разработке CODESYS аспектам безопасности уделяется повышенное внимание. Тем не менее, это не позволяет обеспечить 100%-ю защиту от уязвимостей.

Устранение обнаруженных уязвимостей производится в соответствии с политикой координированного раскрытия компании CODESYS GmbH. Эта политика описывает весь процесс получения информация об уязвимостях, внутренние операции по их устранению и публикацию отчетов для пользователей.

Все поступившие сообщения о нарушениях безопасности тщательно изучаются и оцениваются. Каждой подтвержденной уязвимости присваивается приоритет. Основной целью на данном этапе является определение всех программных продуктов, затронутых уязвимостью, и ее устранение (или выработка временного решения, если исправления не могут быть внесены оперативно). Одновременно с этим производится поиск других уязвимостей в затронутом функционале, в том числе в связанных с ним плагинах и протоколах CODESYS.

Как правило, патчи с устранением уязвимостей выпускаются только для самых последних на данный момент версий CODESYS. При появлении временного решения или выпуске патча публикуются отчеты по уязвимостям. В зависимости от типа и критичности обнаруженной уязвимости стандартный процесс публикации отчетов может отличаться – например, их выпуск может быть ускорен, задержан или вообще отменен. Отчет может быть публичным или рассылаться только OEM-клиентам или отдельным лицам.

Для производителей оборудования (OEM), выпускающих контроллеры со встроенной системой исполнения CODESYS, компания CODESYS GmbH предоставляет доступ к специальной web-странице на сайте CODESYS, посвященной вопросам безопасности. Помимо отчетов по уязвимостям и других документов на данной странице имеется форма подписки на рассылку об уязвимостях. В случае обнаружения уязвимостей OEM-клиенты, подписанные на данную рассылку, информируются с максимально возможной скоростью.

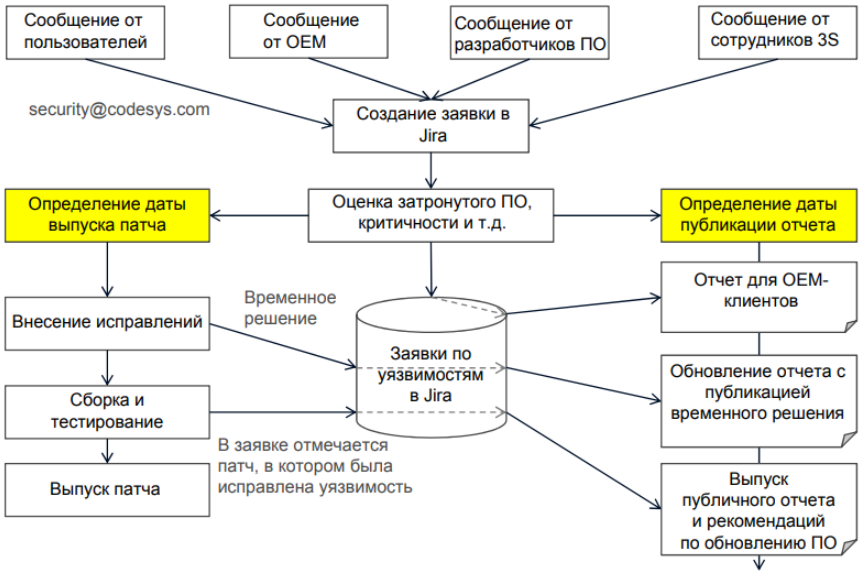

Рис. 4. Структурная схема процесса устранения уязвимостей

9. Заключение

Информационная безопасность промышленных систем управления приобретает все большее значение на фоне повышения степени интеграции различных систем и развития средств связи. Производители оборудования, системные интеграторы и операторы должны уделять повышенное внимание вопросам безопасности. Улучшение систем информационной безопасности должно быть непрерывным процессом с систематической оценкой рисков – таким же, как и улучшение функциональности системы и безопасности обслуживающего персонала. Несмотря на то, что абсолютная безопасность является недостижимой, использование тщательно подобранных средств позволяет поднять уровень безопасности до приемлемого в рамках конкретного промышленного объекта.

10. Отказ от ответственности

Компания CODESYS GmbH не несет никакой ответственности за косвенные, специальные, случайные или побочные убытки, возникающие при распространении (и/или в связи с распространением) и/или использовании данного документа. Вся информация, содержащаяся в данном документе, предоставлена компанией CODESYS GmbH на добровольной основе. Однако, насколько это разрешено законом, ни один из фрагментов документа не закрепляет никаких гарантий, обязательств или ответственности за компанией CODESYS GmbH.

CODESYS® является зарегистрированной торговой маркой CODESYS GmbH. Технические характеристики могут быть изменены. Производитель не несет ответственности за возможные ошибки, неточности, пропуски и опечатки в данном документе.

Примечание: функционал CODESYS может быть ограничен в определенных странах. Для получения подробной информации по поводу географических ограничений следует отправить запрос на адрес support@codesys.com.

11. Список использованной литературы

Самая свежая версия данного документа (*на английском языке*) доступна по ссылке:

https://customers.codesys.com/fileadmin/data/customers/security/CODESYS-Security-Whitepaper.pdf

Стандарт	Название
МЭК 61131-3, 3-я редакция	Контроллеры программируемые. Часть 3. Языки программирования
МЭК 29147	Информационная технология. Методы и средства обеспечения безопасности. Предоставление сведений об уязвимостях
МЭК 30111	Информационные технологии. Методы и средства обеспечения безопасности. Процесс обработки уязвимостей
МЭК 62443	Сети промышленной коммуникации. Безопасность сетей и систем
VDI/VDE 2182	Информационная безопасность в промышленной автоматизации

История версий

Версия	Описание	Дата
1.0	Первая версия документа	21.04.2014
2.0	Добавлено описание функции резервного копирования и восстановления, внедренной в CODESYS V3.5 SP8	28.01.2016
3.0	Добавлено описание средств защиты, внедренных в CODESYS V3.5 SP10. Обновлено описание процесса устранения уязвимостей. Исправлены опечатки	02.01.2017
4.0	Обновлено описание процесса устранения уязвимостей. Добавлен раздел Отказ от ответственности. Расширен список использованной литературы	26.04.2017
4.1	Добавлено описание подписи и шифрования файлов CODESYS IDE	09.05.2017
5.0	Обновлено описание средств безопасности сервера OPC UA	27.06.2017
5.1	Добавлена информация о плагине CODESYS Security Agent	12.12.2017
6.0	Официальный релиз	09.01.2018
6.1	Добавлен п. 5.1.1.1. Проверка целостности проекта. Обновлен п. 5.2.7. Средства безопасности сервера OPC UA. Добавлен п. 5.2.7.2. Сервер OPC UA: управление пользователями. Добавлен п. 5.2.8. Ограничение доступа к символьной конфигурации. Исправлены опечатки.	28.06.2018
7.0	Релиз после проверки и рецензирования	02.07.2018
7.1	Добавлены и исправлены ссылки в п. 5. Обновлены п. 5.2.1 и п. 5.2.6. Добавлен п. 5.1.4	04.05.2020
8.0	Релиз после проверки и рецензирования	10.06.2020
8.1	Уточнены некоторые детали о подписи файлов проектов в п. 5.1.1. Удалена неактуальная информация из п. 5.1.3.	10.08.2020
8.2	Изменен ряд названий, используемых в документе	29.06.2021
8.3	Ряд небольших изменений. Обновлен п. 7. Добавлены п. 5.2.9. Переработаны п. 5.1.3, п. 5.2.1, п. 5.2.7 и п. 5.2.8	17.09.2021
9.0	Релиз после проверки и рецензирования	05.10.2021