BE. services

www.be-services.net

Embedded Security Shield на базе KasperskyOS — встраиваемое защитное решение от «Лаборатории Касперского» и BE.services GmbH

kaspersky

KasperskyOS®

Задача

Для «Лаборатории Касперского» защита АСУ ТП – одно из приоритетных направлений развития бизнеса. Компания тесно сотрудничает с ведущими представителями отрасли, чтобы не просто создать специализированный продукт для решения определенных задач кибербезопасности, но обеспечить новый, более зрелый подход к безопасности каждого аспекта АСУ ТП, будь то SCADA, программируемые логические контроллеры, промышленный интернет вещей, система коммуникаций АСУ ТП, обработка инцидентов и т.д.

В прошлом году «Лаборатория Касперского» совместно с компанией BE.services разработала технологию Embedded Security Shield для повышения безопасности среды разработки CODESYS, широко используемой в программируемых логических контроллерах.

Повышение безопасности среды разработки CODESYS происходит за счет использования компонента Kaspersky Security System (KSS) for Linux, который предоставляет дополнительные гарантии при эксплуатации компонентов CODESYS, отвечающих за коммуникацию с остальной инфраструктурой АСУ ТП. KSS работает поверх операционной системы Linux и использует Linux-контейнеры как изолированные среды для безопасного исполнения потенциально опасных частей ПО.

В данном решении KSS позволяет нейтрализовать большинство векторов атак, с которыми сталкивается любая инфраструктура АСУ ТП. Однако это не стопроцентно безопасное решение в силу того, что в качестве встраиваемой ОС в нем используется Linux, а эксплуатация уязвимости в ядре Linux способна свести на нет даже самую мощную систему защиты, выстроенную поверх нее. Сегодняшние реалии требуют применения новых подходов, не оставляющих киберпреступникам никаких шансов, и при этом не влияющих на другие характеристики АСУ ТП, такие как производительность, рабочие характеристики реального времени и, что немаловажно, общую стоимость системы.

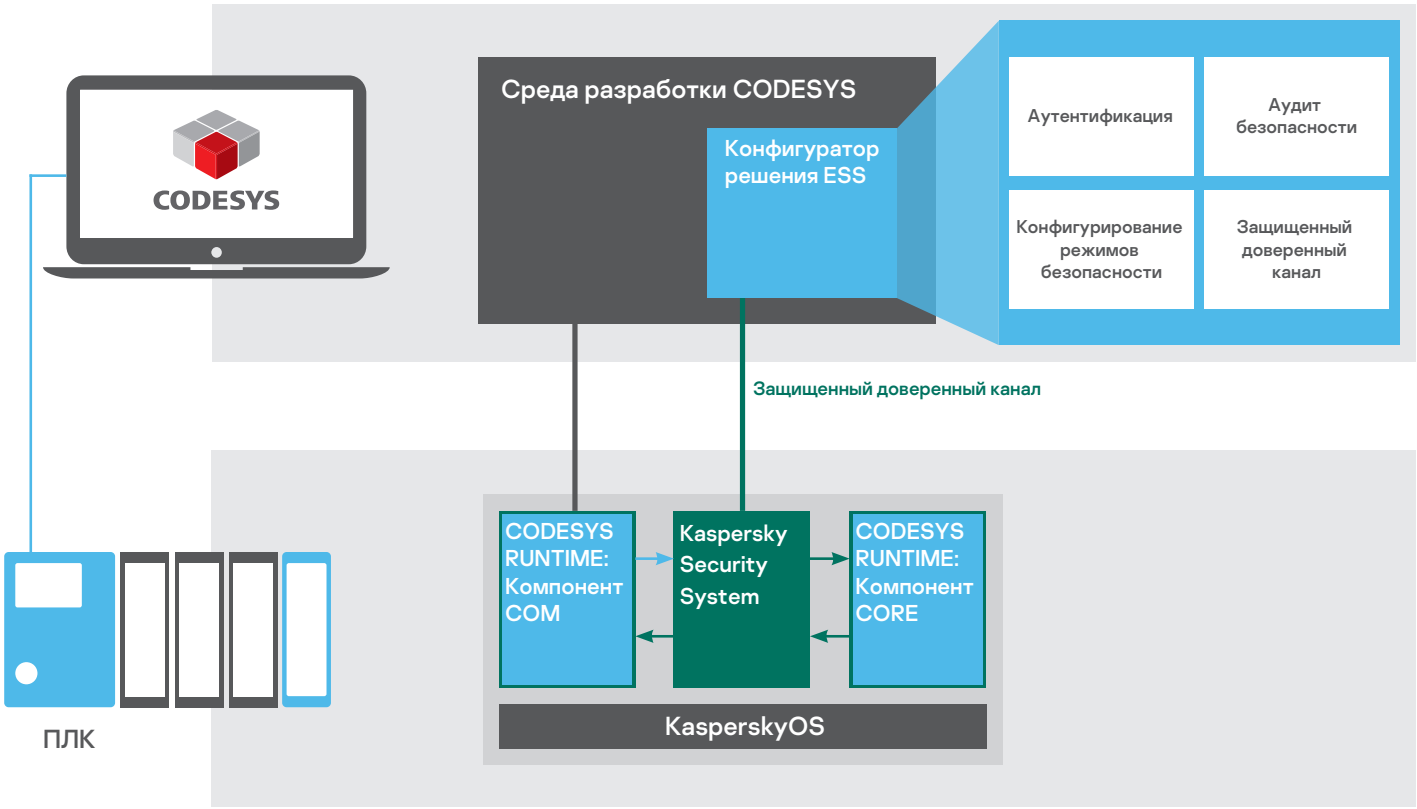
Решение

«Лаборатория Касперского» постоянно совершенствует свои основные технологии, к которым относится KasperskyOS – проприетарная операционная система, способная вывести кибербезопасность АСУ ТП на новый уровень. Существенный прогресс, достигнутый в поддержке требований жесткого реального времени, делает KasperskyOS идеальной платформой для программируемых логических контроллеров.

В этом году «Лаборатория Касперского» в сотрудничестве с BE.services успешно интегрировала среду разработки CODESYS для исполнения под KasperskyOS.

Аналогично Embedded Security Shield, в процессе разработки решения среда CODESYS была разделена на две изолированные части – коммуникационный компонент и основной компонент. Коммуникационный компонент обрабатывает запросы, поступающие из сети АСУ ТП, которая является основной мишенью для кибератак. KasperskyOS обеспечивает надежную изоляцию компонентов ПО, выполняющихся под ее управлением. Это означает, что любая проблема, возникающая в коммуникационном компоненте, не покидает пределов его песочницы и не влияет на остальное решение. KasperskyOS при помощи KSS контролирует все взаимодействия между коммуникационным и основным компонентами CODESYS. KSS анализирует все взаимодействия между компонентами в системе и решает, допустима операция или нет, после чего KasperskyOS обеспечивает исполнение этого вердикта.

Таким образом, взаимодействие коммуникационного компонента с основным компонентом, отвечающим за выполнение программы ПЛК и коммуникацию с оборудованием по промышленной шине, может осуществляться только безопасным способом в строгом соответствии с заданным набором политик безопасности.



«Embedded Security Shield под управлением KasperskyOS – это эксклюзивное решение для обеспечения безопасности устройств интернета вещей и промышленных контроллеров. Мы портировали логический движок CODESYS под KasperskyOS, чтобы обеспечить исходную безопасность и простоту архитектуры системы управления. Экспертиза BE.services в области промышленной автоматизации в сочетании с обширным опытом и знаниями «Лаборатории Касперского» в сфере кибербезопасности позволяют нам предлагать специализированные решения для поставщиков средств автоматизации».

Димитри Филиппе,
генеральный директор
BE.services GmbH

KasperskyOS разработана как исходно безопасная. У нее микроядерная архитектура, а микроядро имеет крайне малую поверхность атаки – оно обслуживает всего три системных вызова. KasperskyOS тесно интегрирована с компонентом KSS, который является ее неотъемлемой частью и поддерживает широкий набор формальных моделей безопасности. KSS предоставляет отдельный, независимый уровень безопасности на самом низком уровне системы, при этом безопасное поведение системы описывается отдельно от бизнес-логики решения.

В результате система становится крайне надежной с точки зрения кибербезопасности. Даже если какой-то из компонентов ПО, работающих под управлением KasperskyOS, будет атакован, это не повлияет на нормальное поведение системы. Более того, движок KSS обнаружит все нарушения политики безопасности, что позволит принять необходимые меры для восстановления этого компонента ПО.

KasperskyOS предлагает готовый расширенный набор механизмов безопасности, включая Доверенный канал (фреймворк на базе протокола TLS), Безопасный аудит, Безопасное обновление и др., которые позволяют надежно контролировать и конфигурировать решение, непрерывно поддерживая его в безопасном состоянии.

Результат

- **Функциональность**
  Предлагаемое решение обеспечивает полноценную работу среды разработки CODESYS. Высокий уровень безопасности не вступает в противоречие с функциональными требованиями.
- **Производительность**
  По результатам внутренних тестов на обширном наборе сценариев, снижение производительности из-за проверок KSS колеблется от 0,5% до 5%. Кроме того, за счет простоты микроядра KasperskyOS и высокой оптимизации драйверов производительность решений на базе KasperskyOS может быть даже выше, чем у аналогичных решений на базе Linux. Что касается требований жесткого реального времени, то согласно результатам тестирования, KSS вызывает минимальные задержки, необходимые для расчетов политик безопасности, которые не влияют на работу решения в режиме жесткого реального времени.
- **Интеграция**
  Реализация среды разработки CODESYS на базе KaspeskyOS полностью совместима с CODESYS IDE, что позволяет сократить время разработки решения и снизить затраты на его внедрение.
- **Безопасность**
  Свойства безопасности решения соответствуют самым жестким современным стандартам для АСУ ТП и при этом не противоречат другим ее характеристикам.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов во всем мире.

О компании BE.services

BE.services GmbH – поставщик встраиваемых программных технологий и сервисов для систем промышленной автоматизации. Специалисты BE.services предоставляют клиентам широкий спектр услуг – от консультирования производителей средств автоматизации при выборе прошивки до решения конкретных задач по разработке решений и реализации проектов «под ключ». Компания BE.services также является системным интегратором и дистрибьютором KasperskyOS – безопасной операционной системы для подключенных к интернету устройств, а также защитного решения KSS для не-CODESYS АСУ ТП.

KasperskyOS®

Подробнее на:
os.kaspersky.ru

www.kaspersky.ru