VERSIONDOG – БЕЗОПАСНОСТЬ В ПРОМЫШЛЕННОСТИ

А.В. Елькин (Компания СФЕРА)

Сформулированы причины рисков потери данных в производственных автоматизированных системах. В качестве возможного пути решения проблемы предложено использовать систему управления программными данными, которая в автоматическом режиме создает резервные копии и производит сравнение с актуальной версией.

Ключевые слова: кибербезопасность, кибератаки, уязвимости, система управления программными данными, резервные копии.

Тесная взаимосвязь между производственными инфраструктурами является основным требованием технологии Industry 4.0. Наличие сложной компьютерной сети имеет свои недостатки, так как значительно облегчает несанкционированный доступ при кибератаке. Многие автоматизированные производства не оборудованы средствами защиты своих компьютерных систем от кибератак. Одним из вариантов по улучшению мер безопасности в автоматизированном производстве является внедрение системы управления программными данными.

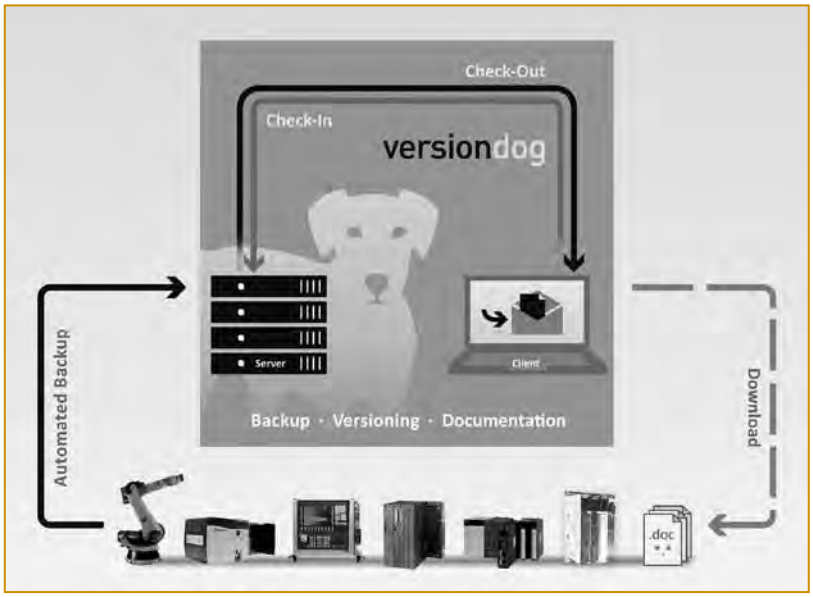

Рис. 1. Последняя версия проекта находится в центральном репозитории, где хранится вся информация

Изначально компьютерные системы автоматизированного производства были созданы закрытыми, так чтобы никто не мог получить доступ извне. Как и раньше, высокая техническая готовность оборудования остается наивысшим приоритетом в сфере производства. Открытие мира промышленных ИТ и их связь с офисными системами стала причиной возникновения определенных трудностей. Конфиденциальность программных данных всегда представлялась важным фактором в работе офисных ИТ, и этот сектор имеет обширный опыт работы с программами по безопасности данных и принятия четких мер защиты. Антивирусные утилиты требуют определенного объема вычислительной мощности и в результате могут замедлить систему. Кроме того, пользователи вынуждены терпеть постоянные обновления и последующие перезагрузки. В сфере автоматизированного производства ситуация немного отличается.

В промышленных ИТ замедление реакции системы на воздействия недопустимо, особенно в системах реального времени с контролем движения. Кроме того, системы производственного контроля (СПК) не имеют механизмов для предотвращения атак вредоносных программ. Согласно исследованию консалтинговой фирмы по управлению предприятиями PricewaterhouseCoopers, число кибератак на производственные объекты компаний в 2014 г. выросло на 48% и составило примерно 42, 8 млн. Почти половина атакованных компаний понесла ущерб. В одной только Германии экономические потери достигли отметки в более чем 51 млрд. евро.

Кибератаки на СПК обычно обнаруживаются на очень позднем этапе. Сами атаки всегда происходят на разных уровнях системы и тем самым не только становятся трудноразрешимыми, но и тесно вплетенными в систему. Конечно, в таких случаях целесообразно внедрение в работу стандартов ISO/IEC 27000, но в большинстве случаев это становится невозможным для

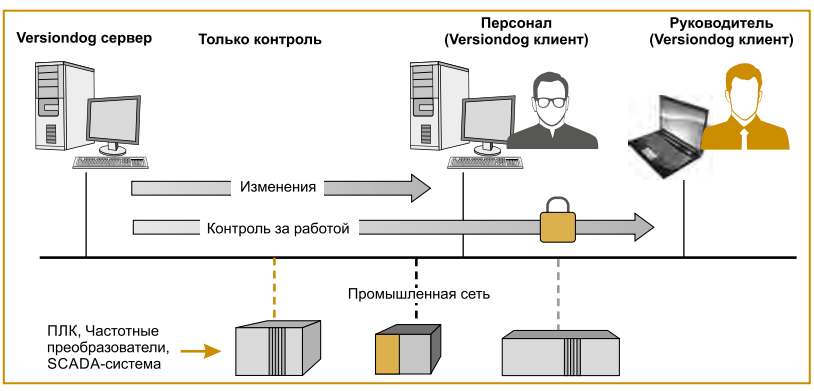

Рис. 2. Структурная схема системы автоматизации, оснащенной системой управления данными

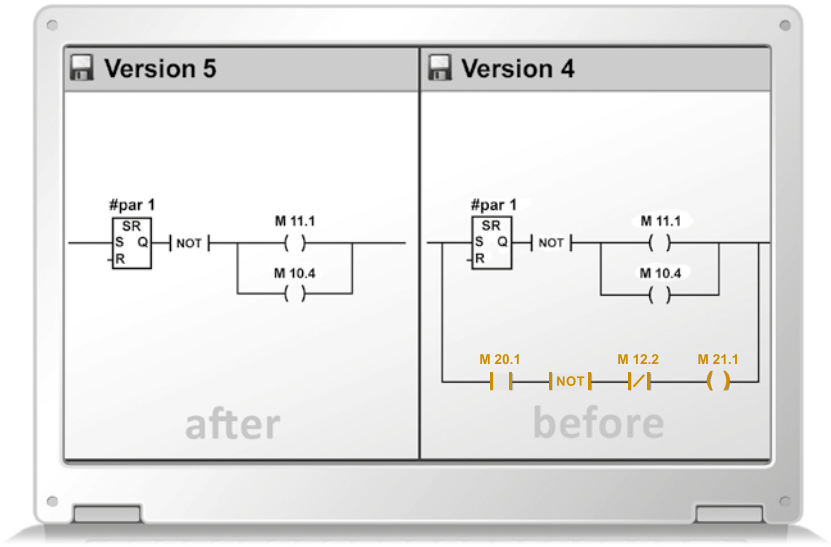

Рис. 3. Обнаружение кибератаки при сравнении последней резервной копии и текущей версии данных

СПК. В целях безопасности первое, что должны сделать компании, это ознакомить сотрудников с потенциальными опасностями, которые могут повлиять на производственную среду. Все работники в обязательном порядке должны быть ознакомлены с основными мерами предосторожности. Далее, может быть обеспечен индивидуальный доступ к программным данным с целью минимизации трудностей при организации рабочих смен персонала или целых отделов.

Другой вариант включает проверку сетевых данных и анализ лог-файлов. Это главная задача операционных центров защиты, которые проверяют программные данные на наличие потенциальных опасностей, чтобы при необходимости отреагировать. Дальнейшие меры безопасности предполагают разделение пирамиды автоматизации на отдельные части с использованием фаерволов. Секторы одного уровня пирамиды также по возможности должны быть изолированы. Это может означать отделение систем безопасности от стандартной системы.

Использование систем управления программными данными в целях защиты программных данных

Одним из выгодных вариантов в работе по улучшению защиты данных является использование системы управления программными данными. Такой тип систем используется в техническом обслуживании электрооборудования при введении в эксплуатацию линий производства и в работе HMI терминалов и SCADA-систем для управления разного типа технологическими процессами (рис. 1). Каждый раз, когда в систему управления оборудованием вводятся актуальные изменения, система управления программными данными сохраняет версию конфигурации данных с примечанием по сделанным изменениям. Тем самым система документирует все изменения программных данных, упрощая процесс контроля за тем, кто изменил что, когда, где и почему. Последняя версия конфигурации программных данных хранится в безопасном архиве, где данные доступны в любое время. Любой неподтвержденный доступ должен рассматриваться как потенциальная кибератака.

Хотя данные меры не предотвращают атаку, они значительно ускорят обнаружение опасности. Сохранение последней неизмененной версии конфигурации программных данных позволяет значительно снизить риски. Рекомендуется проводить ежедневные автоматические проверки данных, например, по окончанию рабочей смены персонала. Масштаб производственного объекта непосредственно связан с объемами программных данных и затрачиваемых усилий, необходимых для проверки всей базы. При наличии на производстве проверенной системы управления программными данными проверка выполняется в автоматическом режиме.

AUVESY.

Компания AUVESY разработала versiondog — систему управления программными данными, которая в автоматическом режиме создает резервные копии данных в автоматизированном производстве.

Программа versiondog сравнивает последнюю резервную копию с предыдущей версией и предупреждает в случае обнаружения изменений. Все программное обеспечение построено на обнаружении различий (функция Smart Compare). Система не только выполняет «умное» двоичное сравнение программных данных, но и выводит результаты на экран в графическом формате, как и в программном обеспечении (рис. 3). Для пользователя это значительно облегчает обнаружение несанкционированного входа в систему. При необходимости можно исключить заданные величины и параметры из списка сравнения данных, чтобы в случае плановой проверки, например, уровня заполнения или разницы температур система не считала это ошибкой.

Елькин Александр Васильевич *– директор компании СФЕРА – официального дистрибьютора компании AUVESY.*
Контактный телефон +7(4725)415779.
E-mail: support@versiondog.ru