



ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ ДЛЯ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

АНИЛ ГОСИН (ANIL GOSINE)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

В последнее время наметилась устойчивая тенденция к тому, что ведущие отраслевые компании, непрерывно совершенствующие деятельность своих предприятий, стремятся обеспечить управление с полным пониманием происходящих процессов, повысить оперативность в принятии решений, улучшить и оптимизировать качество планирования, используя для этого промышленные системы управления (Industrial Control Systems, ICS) и большие данные (Big Data — структурированные и неструктурированные данные огромных объемов и многообразия).

В течение последних десяти лет промышленная автоматизация интенсивно развивалась, благодаря чему сегодня она способна воспринимать и обрабатывать большие объемы данных. В первую очередь это результат технологических инноваций и достижений промышленного «Интернета вещей» (Industrial Internet of Things, IIoT). Однако вместе с тем мы сталкиваемся со следующей проблемой: становится все сложнее выделять и защищать платформы промышленной системы управления (ICS) от внешних и внутренних угроз, поскольку на современных производствах все данные маршрутизируются через сети, а их растущая взаимосвязь приводит к увеличению количества различных сценариев несанкционированного вмешательства в работу предприятий.

Таким образом, исходя из сказанного выше, подходы к решению проблем обеспечения кибербезопасности для защиты предприятий и организаций от угроз и атак также необходимо организовывать для больших данных, осуществляя интеллектуальное управление сетевым трафиком и поведением передаваемых по сетям пакетов. Обычно в интеллектуальных решениях для бизнеса сделан акцент на использование внутренних структурированных данных и аналитической

информации, основанной на определенных правилах, и уже потом эти сведения обрабатываются для принятия того или иного решения. Как следует из самого определения, переход к большим данным приводит к увеличению диапазона и разнообразия поступающей в систему управления информации. В современных системах эти данные могут быть проанализированы, а следовательно, будет получена дополнительная информация о сопутствующих факторах. Благодаря этому мы имеем более тонкое и точное понимание процессов, что позволяет принять оптимальное решение, усовершенствовать выполнение тех или иных процессов и повысить осведомленность о безопасности и наличии или отсутствии угроз.

Большие данные — отнюдь не хаос, по размеру и скорости они масштабируются предсказуемым и простым способом, а потому инструменты отчетности бизнес-аналитики могут развиваться вполне органично. При этом решающее значение, естественно, имеет короткий период ожидания и обработки. Для того чтобы ускорить получение результатов при использовании больших данных, этому процессу следует обеспечить преимущество, добавив возможности просмотра текущей ситуации в режиме реального времени. Таким

образом, в повседневных ситуациях оперативный, инженерный и диспетчерский персонал будет реагировать более гибко и принимать более эффективные решения.

ПРЕИМУЩЕСТВА УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ БОЛЬШИХ ДАННЫХ

Сырые, то есть необработанные и неструктурированные данные, если они потом не превращаются в знания, сами по себе не столь полезны. Поэтому их необходимо анализировать и использовать в интересах лиц, принимающих решения, с учетом конкретного сектора индустрии и архитектуры применяемой сети. Ответом на такую потребность становятся средства программной аналитики и инструменты, подходящие для принятия решений по управлению теми или иными активами, промышленными и технологическими процессами. С точки зрения эффективного применения больших данных для улучшения выпускаемых продуктов и повышения качества и производительности соответствующих процессов, компании могут также визуализировать собранные сведения.

Основной лобой архитектуры сети, работающей с большими данными и использующей их для системы

управления (ICS), является возможность накапливать архивные, или исторические данные, а также инфраструктура, которая дополняет их. Такая архитектура Big Data и сопутствующая инфраструктура служат для агрегирования и представления исторических данных в реальном времени непосредственно в платформу процессов управления для последующей аналитики. Не следует упускать из виду и необходимость иметь надежную инфраструктуру, предназначенную для сбора данных с датчиков, которая должна быть интегрирована в оборудование и системы и обеспечивать возможность их подключения к аналитике больших данных.

Имplementация Big Data и архитектура сети должны гарантировать, что инфраструктура связи с датчиками является достаточно сложной и неоднозначной. Это необходимо, чтобы впоследствии должным образом исследовать и изучать возможные инциденты, происходящие из-за тех или иных нарушений, и не допустить их проявления в будущем. Что касается непосредственно больших данных, их объем определяют сети и связанные с ними функциональные бизнес-единицы. Поскольку все больше секторов индустрии уже использует такие информационные ресурсы, то они, соответственно, смогут создавать больше данных, что со временем станет преимуществом конкретного предприятия при переходе к их конвергенции с системой управления.

Все большее распространение в индустриальном секторе цифровых платформ приводит к тому, что очередная эволюция такой платформы должна найти новые варианты и возможности для промышленных объектов в части сетевого подключения и создания таким путем дополнительной стоимости. Одной из таких платформ является Fieldbus¹, которая считается ключевой технологией средств промышленной автоматизации и позволяет промышленным объектам добиться значительного повышения производительности и, соответственно, экономической эффективности. Капиталоемкий процесс эволюции цифровых платформ в первую очередь нацелен на дорогостоящие производственные активы с длительным жизненным циклом, критические для конкретных отрас-

лей индустрии и, следовательно, на протяжении всего срока эксплуатации требующие постоянного усиленного мониторинга и уже на его основе — прогнозного технического обслуживания.

Цифровые решения Fieldbus выбирают многие компании — исходя из открывающихся благодаря их использованию возможностей для повышения производительности и снижения совокупной стоимости владения объектами (Total Cost of Ownership, TCO), что достигается за счет максимизации применения производственного и технологического оборудования, а также сооружений и объектов инфраструктуры. Это же касается и критериев выбора платформы для работы с большими данными. Такая платформа не должна стать некоей самоцелью, а привести новую ценность благодаря сбору и хранению данных, поступающих от дорогостоящих производственных активов и процессов, в структуре которых она работает. Это также предоставит новые возможности для повышения производительности труда и создания сервисов, основанных на структурированной информации, поступающей в виде больших данных от таких активов и процессов.

Для того чтобы поднять рабочую среду на новый технический и технологический уровень, компании и поставщики решений должны действовать в тесном сотрудничестве. Только так можно гарантировать, что они смогут справиться со всеми трудностями при работе с большими объемами неструктурированных данных, которые уже имеются на многих предприятиях. Они столкнутся с очень большими по объемам журналами регистрации действий операторов, текущими компьютерными логами, журналами событий и метаданными из потоков мониторинга сети и анализа на уровнях пакетов, который также обеспечивает мониторинг в реальном времени, интеллектуальную реакцию и реагирование на инциденты во все более расширяющемся диапазоне потенциальных кибератак.

ТЕКУЩАЯ ОСВЕДОМЛЕННОСТЬ В ЧАСТИ КИБЕРБЕЗОПАСНОСТИ

Непрерывный мониторинг трафика данных, собранных по всей систе-



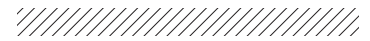
ме предприятия в реальном времени, позволит, например, быстро обнаружить нехарактерную активность или несанкционированную деятельность и сделать это с помощью предварительного моделирования ситуации и машинного обучения в части соответствующего реагирования (рис. 1). Таким образом, владельцы предприятий и аудиторы систем защиты от киберпреступности получают беспрецедентные возможности по обнаружению и точному пониманию проблем устойчивости системы, причем независимо от того, что именно произошло: кибератака, операционный сбой или иной инцидент. В этом случае решения по захвату и анализу пакетов способны проанализировать каждый из них в реальном времени при прохождении захваченного пакета через сеть предприятия. Причем уровни протоколов для передачи пакетов можно разбить так, чтобы можно было определить маршрут, точки назначения и детали по каждому пакету данных.

Анализируя каждый пакет, можно разработать и использовать нормальные шаблоны трафика, позволяющие выявлять отклонения с высокой вероятностью предупреждения их возникновения. Однако существуют проблемы безопасности, исходящие непосредственно от среды получения больших данных, что также необходимо нивелировать с помощью решений, которые обеспечивают защиту и коррелируют с непрерывной эволюцией нереляционных баз данных². Здесь мы имеем в виду меры безопасности для

РИС. 1. ▲
Непрерывный мониторинг трафика данных позволяет, например, быстро обнаружить нехарактерную активность или несанкционированную деятельность

¹ Технология Foundation Fieldbus является цифровой, последовательной, двусторонней системой связи, которая служит базовым уровнем сети в заводских или фабричных системах автоматизации. Это открытая архитектура, которая разрабатывается и осуществляется организацией Foundation Fieldbus. — Прим. пер.

² Нереляционная база данных — термин, обозначающий ряд подходов, направленных на реализацию хранилищ данных, в которых делается попытка решить проблемы быстродействия, масштабируемости и доступности данных за счет их атомарности и согласованности. — Прим. пер.



защиты автоматизированной передачи данных, обеспечивающие высокий уровень проверки достоверности (валидации) информации для подтверждения ее аутентичности, происхождения и точности. Кроме того, необходимо противодействовать извлечению данных для последующего несанкционированного использования, предусмотреть шифрование управления доступом на основе атрибутов и наличие возможностей для подробного аудита, который может управлять таким поистине огромным объемом данных.

ШЕСТЬ ПРЕИМУЩЕСТВ БОЛЬШИХ ДАННЫХ

Поставщики и провайдеры систем управления (ICS), объединяющих разрозненные источники данных в единое целое и анализирующих их через распознавание шаблонов, что позволяет конечным пользователям принимать более эффективные решения, будут определять новую базу для конкуренции и роста бизнеса компаний, что, соответственно, создаст и условия для дальнейшего роста всей мировой экономики. Однако практическая реализация решений с использованием больших данных может быть затруднена, поскольку собранная информация предоставляется с большого числа удаленных узлов сети, датчиков и систем, что может потребовать не только значительных финансовых вложений, но и затрат времени на их импле-

ментацию, а также технических знаний и опыта.

Большие данные можно применить для следующих целей:

1. Сделать информацию более транспарентной (прозрачной).
2. Получить дополнительную детальную информацию об эффективности того или иного производственного и технологического оборудования, что стимулирует инновации и повышает качество конечной продукции.
3. Использовать более эффективную, точную аналитику, чтобы минимизировать риски и заранее обнаруживать проблемы, незаметные до непосредственного их проявления и способные иногда приводить к катастрофическим последствиям.
4. Внедрить те или иные идеи и проанализировать полученные результаты в контролируемых экспериментальных средах и таким образом определить целесообразность конкретных инвестиционных проектов.
5. Обеспечить персонал центра управления (диспетчерской) операционными данными в режиме реального времени, содержащими информацию от систем автоматизации производственных и технологических процессов и аналитику. Это делает управление рисками более эффективным и минимизирует время простоя оборудования, что, в свою очередь, приводит к сокращению персонала управления на 15%

и увеличению выпуска конечной продукции на 5%.

6. Укоренить революционное управление цепочками поставок, прогнозирование спроса, комплексное бизнес-планирование, организацию сотрудничества с поставщиками и эффективный анализ рисков.

ЧТО МЕШАЕТ ВНЕДРЯТЬ НОВЫЕ ТЕХНОЛОГИИ?

В настоящее время мы видим, что еще не все предприятия индустриальной сферы готовы тратить средства на внедрение аналитики с использованием больших данных и извлекать ее преимущества. В рамках недавнего анкетирования, проведенного американским журналом Control Engineering, более четверти опрошенных компаний заявили, что в течение ближайших нескольких лет они не планируют инвестировать в большие данные или «Интернет вещей».

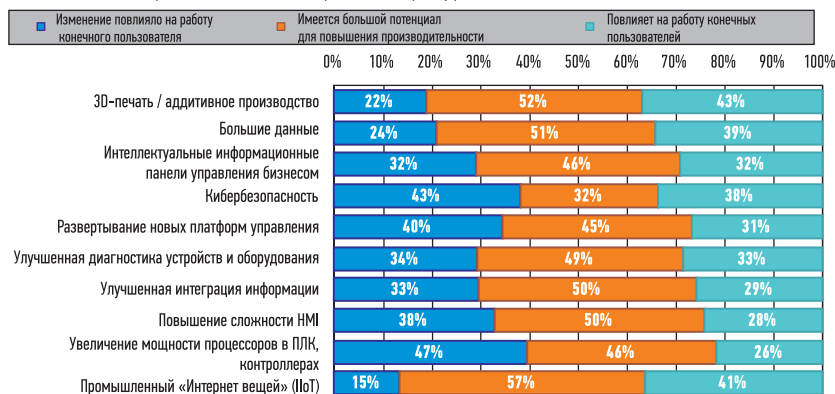
В ходе проведенных исследований (рис. 2) некоторые респонденты отметили, что у них недостаточно знаний для обоснования затрат, связанных с технологией, рассматриваемой в рамках настоящей статьи. Другие ссылались на нехватку ресурсов и времени. Более половины респондентов сообщили, что у них уже есть экономически эффективные и достаточно надежные системы для обеспечения безопасности и роста доходов, а их компании успешно развиваются и без использования больших данных. В то время как сторонники рекламируют большие данные и видят их преимущество в огромном объеме информации, который может улучшить работу предприятий, скептики подчеркивают, что Big Data способствуют расширению зон для кибератак и при отсутствии достаточных защитных слоев негативно влияют на обеспечение кибербезопасности.

Одно из решений проблемы, связанной с повышением отдачи от больших данных, заключается в развертывании мощных визуализаций, охватывающих все доступные данные. Это позволит обеспечить мультиструктурное и итеративное обнаружение нарушений и раскрывает информацию без необходимости направления каких-либо запросов. ●

РИС. 2. ▼
Согласно исследованиям Control Engineering, проведенным в рамках программы оценки влияния промышленного «Интернета вещей» и интеграции информационных технологий, их имплементация может изменить рабочий процесс. Более подробная информация доступна в публикациях, посвященных проблемам Industry 4.0, мобильных вычислений, удаленного доступа к информации, робототехнике, виртуализации и беспроводным сетям, на сайте www.controleng.com/ce-research

Как технологии меняют рабочий процесс

Увеличение мощности процессора в ПЛК и контроллерах общего назначения (47%), решение проблемы кибербезопасности (43%) и развертывание новых платформ управления (40%) - это три главные технологии, которые изменили работу респондентов за последние несколько лет.



Респондентам был задан вопрос: Какая из следующих информационных технологий и тенденций повлияла на вашу работу в течение последних нескольких лет? Что изменит вашу работу в течение следующих нескольких лет? (выборка = 273)