Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760, Остфильдерн,
Германия
Германия
www.pilz.com

«Зоны и каналы» в сетях автоматизации: защита данных обеспечивает безопасность

Безопасность — наш главный приоритет

Ostfildern, июль 2026 г. – **Согласно Машинному регламенту, это является обязательным требованием: информационная безопасность в промышленности призвана защищать функции безопасности от несанкционированного вмешательства, — иными словами, защита данных является необходимым условием для обеспечения работоспособности систем безопасности. Но как обеспечить комплексную защиту сети автоматизации? Стандарты, такие как МЭК 62443-3-2 и готовящийся к публикации EN 50742, определяют четкое направление: разделение систем на зоны и мониторинг подключений — принцип, который проходит красной нитью через все текущие рекомендации отраслевых организаций и экспертов. Компания Pilz убеждена: строгое разделение систем безопасности и так называемой стандартной автоматизации является залогом эффективной безопасности машин, — это основано на принципе эшелонированной защиты и реализуется с помощью подхода, основанного на использовании зон и каналов.**

Дом можно строить таким образом, чтобы он был прочным и безопасным: с крепкими стенами, из огнестойких материалов, с надежной электропроводкой и исправной сигнализацией. Эта конструктивная безопасность является ярким примером безопасности машин, когда конструктивные решения, датчики и

защитные механизмы призваны предотвращать возникновение непреднамеренных опасностей. Однако такой дом остается безопасным только в том случае, если на него не оказывается преднамеренного воздействия. Саботированные регуляторы отопления, поврежденные электрические цепи или отключенные системы сигнализации могут превратить здание, спроектированное с учетом требований безопасности, в источник опасности. В сфере машинного оборудования даже самая совершенная конструкция, обеспечивающая безопасность, теряет свою эффективность, если компоненты, отвечающие за безопасность, подвергаются несанкционированному вмешательству или отключаются без авторизации.

В данном контексте информационная безопасность выполняет роль внешней защиты: прочные двери, надежные узлы подключения, контролируемые соединения и барьеры, препятствующие несанкционированному вмешательству. Таким образом, информационная безопасность не защищает от самих аварий, а предотвращает отключение защитных механизмов, например, со стороны лиц, получивших доступ в результате выбора несанкционированного режима работы или совершения несанкционированных действий. Только так можно обеспечить надежную эффективность мер безопасности — «защита данных для обеспечения безопасности».

От нормативных требований к предлагаемому решению

Впервые Машинный регламент (ЕС) 2023/1230 устанавливает информационную безопасность в качестве обязательного требования к функциям безопасности установок и машинного оборудования: функции безопасности не должны нарушаться в результате манипуляций, будь то умышленных или иных.

Именно здесь на помощь приходит разрабатываемый стандарт EN 50742; он поможет прояснить основные требования к информационной безопасности, заложенные в Машинном регламенте. Данный стандарт определяет технические характеристики мер защиты от вредоносных действий и устанавливает четкие требования к аппаратному и программному обеспечению, а также к данным, которые могут влиять на функции безопасности. Данный стандарт охватывает весь жизненный цикл — от разработки до эксплуатации и вывода из эксплуатации. Ключевую роль играет также действующая серия стандартов МЭК 62443, в которой изложен системный подход к кибербезопасности систем автоматизации и управления. Он обеспечивает структурированную основу для анализа рисков, «эшелонированной защиты» и принципа сегментации («зоны и каналы») и прямо признан в стандарте EN 50742 в качестве альтернативного или дополнительного подхода к обеспечению информационной безопасности. В совокупности эти стандарты составляют нормативную основу концепции «Защита данных для обеспечения безопасности»: они предписывают признавать цифровую целостность машины обязательным условием ее функциональной безопасности и обеспечивать ее соответствующую защиту.

Почему «зоны и каналы» повышают безопасность машинного оборудования

Вернемся к образу дома: котельная символизирует зону, а подключение к шлюзу «умного дома» — соответствующий канал. Если это подключение подвергнется взлому, это может повлиять на работу всей системы — даже если само помещение надежно защищено. Поэтому крайне важно обеспечить информационную

безопасность не только отдельных зон, но и маршрутов, соединяющих их. Именно здесь и приходит на помощь принцип «зон и каналов». Зоны четко отделены друг от друга, а переходы между ними оборудованы средствами контроля. Подобно тому, как в доме двери и присвоенные им ключи определяют, кто и куда может пройти, на промышленном предприятии внутренние меры защиты (безопасность) и внешняя защита от несанкционированного вмешательства (защита данных) структурно взаимосвязаны.

В результате обеспечивается концепция защиты, основанная на принципе эшелонирования: безопасность обеспечивается не за счет одного барьера, а за счет нескольких уровней защиты, расположенных один за другим. Если один барьер преодолен, следующий остается на месте. Эти многоуровневые пространства образуют зоны, а каналы — это контролируемые проходы между ними. Таким образом, одна уязвимость не может поставить под угрозу всю систему, особенно когда речь идет о безопасности и, следовательно, о защите людей.

Компания Pilz последовательно придерживается подхода «Защита данных для обеспечения безопасности», при этом безопасность является основной целью защиты данных. Основное внимание уделяется защите данных в сфере безопасности, что, в свою очередь, обеспечивает защиту людей.

Именно поэтому компания Pilz отделяет систему безопасности от общего управления машиной, то есть от стандартной автоматизации, тем самым снижая риск воздействия на функции, связанные с безопасностью. Чем четче функционально разделены эти «защищаемые активы», тем меньше дополнительных мер безопасности требуется для обеспечения надежной защиты.

Преимущества такого подхода очевидны на протяжении всего жизненного цикла оборудования. Если функции безопасности и стандартные функции разделены, нет необходимости проводить повторную сертификацию или адаптировать функции безопасности параллельно с обновлением стандартных функций. Это позволяет значительно сократить объем работ по техническому обслуживанию и ремонту. Кроме того, классические системы обеспечения безопасности требуют значительно меньшего количества обновлений, критически важных для безопасности, по сравнению со стандартными системами управления, поэтому такое разделение позволяет избежать многих ненужных вмешательств. Разделение также дает технологические преимущества: автономная система безопасности, такая как компактный контроллер PNOZmulti 2, может свободно сочетаться с системами управления от разных производителей, в то время как встроенные системы зачастую привязаны к конкретным технологиям. В то же время использование отдельных систем безопасности повышает сложность задачи для злоумышленников, поскольку каждую систему приходится взламывать по отдельности, что значительно затрудняет манипуляции. Более того, стандартная система может работать в сетевом режиме по мере

необходимости, в то время как собственно функции безопасности остаются изолированными, что позволяет значительно сократить уязвимую поверхность.

Такое разделение систем автоматизации по безопасности и защите данных — каждая из которых имеет четко согласованные уровни информационной безопасности — также повышает эффективность, упрощая планирование мер по обеспечению безопасности, техническому обслуживанию и расширению. Таким образом, изменения в стандартной программе не требуют каких-либо изменений в разделе, связанном с безопасностью, что значительно сокращает объем необходимых работ по программированию и адаптации. В то же время такое разделение имеет положительное влияние на расходы на программное обеспечение и техническую поддержку, поскольку при использовании отдельных систем затраты на лицензии и обслуживание зачастую оказываются ниже.

Защита благодаря разделению — профессионализм благодаря обучению

Четкое разделение систем безопасности и стандартной автоматизации не только обеспечивает техническую надежность, но и снижает вероятность ошибок оператора, а также уменьшает потребности в обучении. Поскольку функции безопасности выполняются на выделенном аппаратном обеспечении и четко отделены в организационном плане, они остаются защищенными даже в случае внесения изменений в стандартную программу. В результате ошибки в повседневной работе не ставят под угрозу безопасность, а обязанности можно распределять более четко.

Компания Pilz предлагает комплексную программу обучения и сервисного обслуживания, призванную помочь предприятиям внедрить эту архитектуру. К ним относятся учебные курсы «Основы информационной безопасности в промышленности» и «CESA — Certified Expert for Security in Automation», а также услуги в области информационной безопасности в промышленности. В них объясняется, как на основе отдельных элементов схемы разрабатывать надежные концепции «Защита данных для обеспечения безопасности», но при этом они выходят далеко за эти рамки: они демонстрируют, как систематически управлять рисками безопасности и разрабатывать комплексные концепции безопасности, как учитывать требования стандарта МЭК 62443, как структурировать архитектуру безопасной сети машин, а также как оценивать и непрерывно повышать эффективность принимаемых мер.

Одно из ключевых преимуществ этого подхода заключается в том, что операторам на стороне конечного пользователя не требуется глубоко вникать в вопросы безопасности, поскольку защита функций безопасности уже обеспечена за счет архитектурной конструкции системы. По этой причине учебные курсы в первую очередь предназначены для тех, кто принимает решения в области информационной безопасности или разрабатывает системы, в то время как операторы могут продолжать работать в безопасных условиях без необходимости прохождения дополнительного обучения по информационной безопасности в промышленности. В результате достигается четкое распределение ролей, которое упрощает эксплуатацию

установки и одновременно обеспечивает устойчивое повышение уровня безопасности.

Повышенная безопасность благодаря четкой структуре — и соответствующему опыту

Эффективная стратегия «Защита данных для обеспечения безопасности» достигается не за счет отдельных мер, а благодаря продуманной архитектуре, четкому распределению обязанностей и целенаправленному развитию профессиональных навыков. Именно здесь на помощь приходит компания Pilz. Благодаря строгому приверженности принципу эшелонированной защиты и четкому разделению систем безопасности и стандартной автоматизации, Pilz закладывает основу для создания отказоустойчивого машинного оборудования — а также предлагает практическое обучение и консультационные услуги, чтобы компании могли уверенно двигаться по этому пути. В результате достигается уровень безопасности, который не только соответствует требованиям стандартов, но и обеспечивает ощутимую дополнительную выгоду в повседневной работе: более простой, надежный и эффективный в долгосрочной перспективе.

((Количество знаков: 9 640))

Компания-технологический лидер предлагает комплексные решения по автоматизации для обеспечения промышленной и информационной безопасности машинного оборудования. Сюда входят датчики, системы управления и приводная техника, а также устройства для промышленной связи, диагностики и визуализации. В международный спектр услуг также входят консультирование, инжиниринг и обучение. Помимо машиностроения, решения Pilz используются во многих отраслях, например, во внутренней логистике, упаковочной промышленности и на железнодорожном транспорте, или в робототехнике.

www.pilz.com

Компания Pilz в социальных сетях:

На наших каналах в социальных сетях мы предоставляем справочную информацию о компании и людях, которые работают в Pilz, а также информируем о последних новостях из области автоматизации.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Контактные лица для прессы:

Мартин Курт

Корпоративная и техническая пресса
Тел.: +49 711 3409-158
m.kurth@pilz.de

Сабина Каррер

Техническая и корпоративная пресса
Тел.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Дженни Скарман

Техническая пресса

Телефон: +49 711 3409-1067
j.skarman@pilz.de

Ева Гельнер-Рёссле

Техническая пресса

Тел.: +49 711 3409-7147
e.roessle@pilz.de