22.07.2026

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Германия
https://www.pilz.com

Сообщение для Прессы

Защита данных в целях обеспечения безопасности: четкие структуры в сети автоматизации

Остфильдерн, 22.07.2026 - **Андреас Виллерт, руководитель отдела информационной безопасности в промышленности, Pilz Австрия**

(«Возможны изменения»)

В Машинном регламенте (ЕС) 2023/1230 четко оговаривается, что система безопасности может надежно функционировать только в том случае, если функции, связанные с безопасностью, защищены от несанкционированного вмешательства. Современное машинное оборудование объединено в цифровую сеть, настраивается с помощью программного обеспечения и регулируется в процессе работы. Любое несанкционированное изменение — будь то преднамеренное или случайное — может привести к утрате эффективности защитных мер.

Именно поэтому информационная безопасность уже не является просто дополнительным фактором, а представляет собой основное условие надлежащего функционирования системы безопасности. Цель состоит в том, чтобы обеспечить целостность всех компонентов, связанных с безопасностью, с тем чтобы функции безопасности срабатывали именно тогда, когда это необходимо.

Как стандарты и архитектурные принципы обеспечивают надежную безопасность
Серия стандартов МЭК 62443 и разрабатываемый стандарт EN 50742 создают четкую структуру для этого. И то, и другое требует создания систематизированной архитектуры безопасности, которая обеспечивает оценку рисков, строит защитные меры в структурированном виде и имеет четкое разделение системы на сегменты.

В основе системы лежит принцип «зон и каналов»: системы разделяются на зоны, а переходы между ними контролируются. Такой подход обеспечивает эшелонированную защиту, то есть многоуровневую стратегию безопасности, в рамках которой несколько уровней защиты дополняют друг друга и значительно затрудняют несанкционированное вмешательство.

В соответствии со стандартом МЭК 62443 компания Pilz выступает за строгое разделение систем безопасности и стандартной автоматизации. Функции безопасности осуществляются отдельными аппаратными средствами и изолированы как организационно, так и технически. Это означает, что на них не влияют обновления, ошибки или атаки, возникающие в стандартной системе автоматизации. Площадь атаки сокращается, как и объем работ по техническому обслуживанию.

Ключевым фактором успеха в данном случае является степень изоляции: чем больше разграничение между функциями безопасности и производственной сетью, а также сетью оборудования, тем лучше они защищены. В то же время снижается потребность в дополнительных мерах информационной безопасности.

Поэтому проверенным способом является перенос приборов, выполняющих функции безопасности, в отдельный сегмент сети. Крайне важно правильно настроить этот сегмент с помощью политик доступа и дополнительных механизмов аутентификации. Поскольку системы безопасности отличаются высокой стабильностью по сравнению с стандартными средствами автоматизации и редко подвергаются изменениям, такую строгую сегментацию можно эффективно реализовать как с точки зрения эффективности, так и с точки зрения информационной безопасности. Однако важно, чтобы принятые меры последовательно соблюдались на протяжении всего срока службы машины.

Доступность диагностических данных играет особенно важную роль, в частности, в случае крупногабаритного машинного оборудования или сложных производственных комплексов. В случае неисправности необходимо быстро выяснить, по какой причине сработала функция безопасности: было ли задействовано аварийное отключение — и если да, то какое именно средство? Произошло ли прерывание работы световой завесы — и в какой точке? Или, возможно, в электрической схеме произошло короткое замыкание? Такая информация помогает значительно сократить время простоя и быстро возобновить работу установки. Диагностические данные касаются не только того, «что сломалось», но, прежде всего, того, «что именно произошло».

В четко сегментированной архитектуре тем не менее возможно передавать данные диагностики безопасности на стандартный ПЛК, — при условии, что доступ к самим функциям безопасности в пределах их защищенной зоны остается строго запрещенным.

Для простых ситуаций подходящим решением станут реле безопасности из линейки PNOZ, а для более сложного машинного оборудования рекомендуется индивидуальная реализация с использованием myPNOZ. Эти устройства не поддерживают сетевые функции и, следовательно, не имеют уязвимостей для удаленных атак. Это позволяет значительно сократить как объем работ по разработке, так и требования к мерам информационной безопасности при эксплуатации. Компания Pilz также предлагает комплексную программу обучения и сервисного обслуживания — от основ промышленной безопасности до сертификации CESA. В данном материале объясняется, как разрабатывать безопасные архитектуры, оценивать риски и совершенствовать меры безопасности на основе принципов устойчивого развития. В результате мы получаем компетентность именно там, где она необходима: среди тех, кто занимается планированием, проектированием и несет ответственность за системы.

Что на самом деле дает такой подход

Разделение систем безопасности и стандартной автоматизации дает множество преимуществ на протяжении всего жизненного цикла машины:

- Повышенная безопасность: функции безопасности защищены от несанкционированных изменений — независимо от того, что происходит в системе стандартной автоматизации.
- Меньше усилий: обновления, сертификации и корректировки не нужно выполнять повторно.
- Меньшая сложность эксплуатации: операторам не требуется глубоких знаний в области информационной безопасности; архитектура автоматически обеспечивает безопасность.
- Повышенная гибкость: независимые системы безопасности, такие как PNOZmulti 2 или myPNOZ, могут интегрироваться в оборудование различных производителей.
- Снижение затрат: меньше поддержки, меньше лицензий, меньше вмешательств — и, следовательно, низкая совокупная стоимость владения.

Компания Pilz объединяет надежные технологии, четкую организационную структуру и целенаправленное обучение в рамках стратегии «Защита данных в целях обеспечения безопасности», которая соответствует требованиям стандартов и действительно облегчает повседневную работу: она безопасна, понятна и эффективна в долгосрочной перспективе.

Надпись:

Тексты и изображения для скачивания вы можете найти по адресу:
https://www.pilz.com/ru-INT/company/press/messages/articles/249002

Pilz — Дух безопасности

Компания Pilz является мировым поставщиком изделий, систем и услуг в области автоматизации. Будучи флагманом в области безопасной автоматизации, компания Pilz обеспечивает безопасность для человека, оборудования и окружающей среды. Основанная в 1948 году, сегодня семейная компания с головным офисом в Остфильдерне — это 2500 сотрудников в 42 дочерних компаниях и филиалах.
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.

Компания Pilz в социальных сетях

Через наши социальные медиа-каналы мы предоставляем справочную информацию о компании Pilz и ее сотрудниках. Мы также информируем о текущих событиях в области автоматизации.


https://www.facebook.com/pilzINT


https://www.youtube.com/user/PilzINT


https://www.linkedin.com/company/pilz


https://pilz-magazine.com/en/

Контактное лицо для журналистов

Martin Kurth
Корпоративная и Техническая пресса
+49 711 3409 - 0
publicrelations@pilz.com

Sabine Skaletz-Karrer
Техническая пресса
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de