19.05.2022

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

Сообщение для Прессы

Томас Пильц: Дух защиты в цифровой автоматизации

г. Остфильдерн, 19.05.2022 - **(«возможны изменения»)**

Защита машинного оборудования – от требования к средствам, облегчающим взаимодействие
С начала промышленной революции и до начала прошлого века главное, что требовалось от машин, это производительность. Человеческий труд стоил дешево, что, к сожалению, означало отсутствие стимула для инвестиций в защитные меры. Защита машинного оборудования в том виде, в котором мы знаем ее сегодня, возникла не ранее 40 лет назад. В 1986 году были внесены изменения в Директиву по машинному оборудованию, и с этого момента обеспечение защиты машинного оборудования в Европе стало обязательным.

До этого момента самым простым способом обеспечения защиты было физическое разделение. Были установлены защитные ограждения, которые позволяли рабочим управлять прессом только при помощи клавиатуры. Такое решение устраняло риск травм, но также снижало чувство удовлетворенности от работы и ухудшало эргономику.

В 1987 году, то есть 35 лет назад, благодаря изменениям в Директиве по машинному оборудованию, компания Pilz вывела на рынок реле **PNOZ (Pilz Not-Aus zwangsgeführt)**, что в переводе с немецкого означает «устройство аварийного останова с принудительным управлением». Это было первое защитное реле, которое обеспечивало останов машины в случае опасности. Меньше, чем обычная электронная схема, проще в эксплуатации и, прежде всего, защищеннее благодаря сертифицированному типовому испытанию - как раз то, что нужно в эпоху, когда защита машин становится все более важной, в том числе и с точки зрения законодательства, при этом требуется максимально упростить процесс внедрения таких мер защиты операторами установок. На начальном этапе защита машин реализовывалась с помощью PNOZ. Сегодня PNOZ - это синоним защитного реле.

Безопасная автоматизация в том смысле, в котором мы понимаем ее сегодня, существует только с 1995 года, когда компания Pilz выпустила первый свободно программируемый защитный контроллер PSS 3000. С этого момента появилась возможность использовать электронные контроллеры в технологии обеспечения защиты. Раньше это было прямо запрещено. Требования законодательства удалось изменить только после трудных переговоров с федеральными министерствами и европейскими комитетами.

А как обстоит дело сейчас? Используя Европейскую Директиву по машинному оборудованию и североамериканские стандарты OSHA и UL в качестве образцов, в последние годы специалисты начали работу по формированию **глобальной сети стандартов защиты**. Этот процесс чрезвычайно далек от завершения. Но все больше и больше компаний приходят к пониманию того, что, помимо заботы о человеке, защита имеет и экономическую ценность. Мы благодарны за прошлые и нынешние возможности внести свой вклад в это позитивное развитие,

которое продолжается и сегодня: Во многих областях защитные промежутки между человеком и машиной сокращаются, так как они вместе выполняют задачи на одних и тех же рабочих местах. Защита становится фактором, способствующим совместной работе человека и робота. Кроме того, наши решения по защите также способствуют повышению производительности за счет увеличения эксплуатационной готовности установок и машин. Таким образом, наши решения полностью соответствуют потребностям инженерного искусства, направленного на повышение производительности машин, а также потребностям тех, кто использует их. Такие области, как цифровизация и безопасность, формируют новые вызовы в защите человека и машины. Сегодня мы представим некоторые ответы, которые компания Pilz дает на эти вызовы, выступая под лозунгом **«Дух защиты в цифровой автоматизации»**.

Защита и безопасность идут рука об руку
Машиностроение и промышленность имеют хорошие позиции в вопросах защиты, чего, к сожалению, нельзя сказать о безопасности. Безопасность более не может быть темой, которой можно заниматься только тогда, когда есть свободное время. Напротив, в настоящее время это, возможно, самая важная и актуальная тема в инженерии и даже в промышленности в целом. Промышленная информационная безопасность ранее входила в задачи сферы информационных технологий (ИТ) в форме безопасности информационных технологий. В наши дни производственные и промышленные предприятия также обладают чрезвычайно развитыми ИТ-системами. Мы называем это ОТ (эксплуатационные технологии), или промышленная безопасность. Под этим термином понимается защита производственных и промышленных предприятий от намеренных или случайных сбоев. Задача промышленной безопасности состоит в том, чтобы гарантировать эксплуатационную готовность машин и оборудования, целостность и конфиденциальность данных и технологического процесса оборудования.

В конечном счете, если я не контролирую свои данные, то под угрозой оказывается компания и защита моих сотрудников: без безопасности нет защиты, а это значит, что люди подвергаются риску!
Компания Pilz полагает, что отсутствие рисков людей и оборудования может гарантировать только комплексный подход к безопасности и защите. Поэтому внедрение мер безопасности непосредственно в устройствах (например, контроллерах) также является абсолютно необходимым. При этом необходимо анализировать весь жизненный цикл системы, то есть обеспечение безопасности начинается с момента разработки.
Вот уже около 20 лет наш отдел управления функциональной защиты (FSM) занимается проверками и сертификацией защиты. Кроме того, в течение последних нескольких лет компания Pilz выстраивает применяемые ей процессы разработки в соответствии со стандартом IEC 62443-4-1 «Безопасность систем промышленной автоматизации и управления. Часть 4-1. Требования к жизненному циклу разработки безопасной продукции», что позволяет наглядным образом подтвердить безопасность разработки. Этот факт был сертифицирован компанией TÜV Süd в ходе аудита. В стратегическом плане сертификация не менее важна, чем сертификация функциональной защиты.

От безопасного изделия к безопасному применению

Я хотел бы показать вам, как может выглядеть безопасная машина в 2022 году.

Безопасный доступ к процессу для выбора режима работы

Для защиты от несанкционированного доступа на объекте предусмотрена система выбора режима работы и управления правами доступа PITmode. При помощи RFID-ключей операторы могут надежно контролировать индивидуальные разрешения на доступ, в соответствии с установленными требованиями.

Доступ технологического процесса к HMI и системам управления
Операторские панели PMI (человеко-машинный интерфейс Pilz) используются операторам для мониторинга и управления технологическими процессами. Компания Pilz предлагает PASvisu - веб-решение для визуализации оборудования и машин.

Физический доступ через ограждение или двери
Защита персонала и технологического процесса при помощи ограждений и дверей для доступа Системы защитных ограждений компании Pilz обеспечивают защиту от опасных движений и вылета деталей машин, останавливая перемещение оборудования. Эти системы можно использовать с технологией безопасного управления, например, с защитным реле myPNOZ или конфигурируемым безопасным компактным контроллером PNOZmulti 2.

Удаленный доступ к HMI и системам управления
Межсетевой экран SecurityBridge предотвращает несанкционированные действия с данными. Работая в сети управления, он защищает соединения между инструментами диагностики или настройки и контроллерами от несанкционированных действий и устанавливает защищенные соединения с внешней средой. Передача данных осуществляется почти без задержек.
В будущем наш портфель услуг по защите и безопасности будет дополнен услугами по обеспечению промышленной безопасности, о которых моя сестра расскажет позже.

Мировые стандарты защиты и безопасности
Вопросы цифровизации и безопасности требуют адаптации существующих стандартов и директив, а также разработки новых. Европейская директива по машинному оборудованию остается важным фактором дальнейшего развития защиты машин: в настоящее время выполняется ее пересмотр, чтобы составить новый Регламент ЕС по машинному оборудованию. При этом, в частности, затрагиваются вызовы, которые могут возникнуть в процессе цифровизации. Таким образом, определение компонентов обеспечения

защиты теперь также включает программное обеспечение, если оно выполняет функции защиты. Параллельно с проектом данного документа, подготовленного Еврокомиссией, опубликован отдельный проект регламента Евросоюза по искусственному интеллекту. Он посвящен всем изделиям с ИИ и их применению. С выходом нового Регламента по машинному оборудованию учет вопросов безопасности также становится обязательным. Были пересмотрены или в настоящее время пересматриваются основные стандарты функциональной защиты при проектировании и строительстве машин. Летом ожидается публикация стандарта ISO 13849, в котором будет уделяться большее внимание ПО и требованиям к нему. Стандарт IEC 62061 был опубликован в 2021 году и затрагивает, в частности, тему безопасности.
Ключевое слово: безопасность В настоящее время в Германии разрабатывается новый закон по информационной безопасности. На европейском уровне в настоящее время идет пересмотр Директивы по обеспечению высокого уровня сетевой и информационной безопасности (Директива NIS), чтобы в итоге разработать Директиву NIS2 и Закон об устойчивости к угрозам кибербезопасности, а также ведется работа над рядом нормативных актов, которые уже являются абсолютно обязательными в Китае. Ранее Директива NIS касалась только «ключевых субъектов», то есть критически важных элементов инфраструктуры. Область применения Директивы NIS2, выход которой ожидается в 2024 году, расширена до «важных субъектов». В этом случае речь пойдет, например, о европейских машиностроительных предприятиях, если у них имеется 50 и более сотрудников или годовой оборот составляет 10 млн евро. По оценкам Германской федерации машиностроителей (VDMA), под действие этой Директивы в Европе подпадут около 9 000 компаний, включая Pilz.
Таким образом, машиностроители могут столкнуться с новыми и порой чрезвычайно строгими законодательными требованиям в отношении безопасности. Однако в настоящее время они

совершенно не знают об этом. Это касается как работы информационных систем (безопасность информационных/эксплуатационных технологий), так и сетевых систем (компоненты, установки, машины).

В других странах законодательные требования к безопасности также ужесточаются. Например, в Китае ситуация обстоит следующим образом: в сентябре 2021 года вступили в действие «Закон о безопасности данных» (DSL) и «Положение об управлении уязвимостями безопасности сетевых продуктов». Последний документ более четко определяет методы и правила подачи отчетности и обязательства («Раскрытие информации») в случае обнаружения уязвимостей в безопасности изделий. С 1 ноября 2021 года действует «Закон о защите личной информации», аналогичный по смыслу европейскому Общему регламенту о защите данных (GDPR). Иностранные компании, собирающие данные в Китае, также подпадают под действие этого Положения.

В качестве «посла защиты» компания Pilz на протяжении десятилетий интенсивно работает над формированием действующих стандартов и участвует в разработке директив. Мы предлагаем на рассмотрение вопросы, возникающие в ходе практической работы. Более 30 экспертов компании Pilz активно участвуют в работе примерно над 100 стандартами защиты изделий и их применения в почти 80 комитетах по стандартизации по всему миру, в том числе в китайском комитете по стандартам «SAC/TC 208 Национальный технический комитет по защите машин Управления стандартизации Китая», который играет важнейшую роль в разработке стандартов по защите машин. Компания Pilz стала первой иностранной организацией, ставшей членом этого комитета – это произошло в 2004 году.

Надпись: *Томас Пильц, управляющий партнер (фото: © Pilz GmbH & Co. KG)*

Тексты и изображения для скачивания вы можете найти по адресу:
https://www.pilz.com/ru-INT/company/press/messages/articles/232049

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://twitter.com/Pilz_INT

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


https://www.xing.com/companies/pilzgmbh%26co.kg

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

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