УДК 004.51

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП И КФС В SMART FACTORY

Авторы:
Уляхин А.А., Университет ИТМО, Санкт-Петербург
ulahin.alex@niuitmo.ru
Викснин И.И., Университет ИТМО, Санкт-Петербург
wixnin@cit.ifmo.ru
Научный руководитель – к.т.н., доцент факультета БИТ
Птицын Алексей Владимирович, Университет ИТМО, Санкт-Петербург
pav@cit.ifmo.ru

Анализ факторов влияющих на обеспечение информационной безопасности в АСУ ТП при внедрении современных информационной технических систем и трансформации в кибер-физические системы цифрового производства. Результаты могут быть использованы при разработке модели обеспечения безопасности модели организации защищенного цифрового производства.

В рамках непрерывного совершенствования средств автоматизации и наступления эпохи четвертой промышленной революции компании встречаются с новыми требованиями к обеспечению безопасности. Сфера автоматизации сливается со сферой ИТ и для работы предприятий, созданных по концепции Индустрии 4.0, особую важность приобретают такие фундаментальные аспекты как безопасность на производстве и информационная безопасность. В отличие от производств традиционного типа цифровые производства смешивают процессы в физической и цифровой среде.

В первую очередь нужно понимать, что кибер-физические системы (КФС) не является отдельной от автоматизированной системы управления технологическими процессами (АСУ ТП) структурой, они неразрывно связанны. КФС базируется на АСУ ТП. Но, будучи результатом взаимной интеграции, они так же неразрывно связаны с информационно-технологические системы (ИТС). Поэтому, сравнение АСУ ТП и КФС будет рассматриваться как различия базовых компонентов КФС.

В информационных системах первостепенную важность имеют отдельные объекты, в частности информация и каналы связи. Упор делается на информационную безопасность. Это связанно с тем, что ИТС процессы являются распределенными и чаще всего, технологическая цепочка не нарушается при отказе или недоступности одного из звеньев. Нарушение работы канала связи может быть восстановлено или задублирована, без нарушения работы оконечных объектов, а потерянная информация замедляет лишь два связанных между собой объекта или они и вовсе могут быть перенаправлены на выполнение других процессов, до момента восстановления.

В свою очередь, для АСУ ТП приоритетным является сам процесс. Упор делается на функциональную безопасность. Поскольку любое производство строится из последовательных производственных цепочек, то нарушение работы или недоступность одной из них может остановить производство, до полного восстановления. При этом, поскольку объекты АСУ ТП, находятся в прямой физической зависимости между собой и выходи из строя одного процесса может непосредственно повлиять на работу другого процесса.

Для большей наглядности привожу перечень возникающих вопросов при формировании КФС на базе обобщенной ИТ системы и АСУ ТП:

- Системы реального времени и критичность реакций
- Контроль доступа на основании политик ИБ и человеко-машинного интерфейса

— Обеспечение резервирования процессов и однозначное описание действий в случае отказа
— Разность критичности простоя узла и бизнес-процесса
— Медленное и ограниченное или невозможность развития, специализированного ПО, протоколов коммуникации ЭВМ и ОС
— Возможности обновления и коррекции ПО в рамках бесперебойного производства
— Обеспечение децентрализованной поддержки ПО и оборудования
— Организация физического доступа исходя из сложной топологии производства и особенностей оборудования

Все больше и больше организаций проходит процесс трансформации в цифровое производство. Зачастую это происходит в виде слияния двух различных, развитых независимо, систем. Хотя все факторы риска, связанные с ИТ, применимы к системам АСУ ТП, крайне сложно полностью наложить структуру безопасности ИТС на системы АСУ ТП.