Заключение на соответствие системы мониторинга температуры и влажности «RapidSCADA» главе 21 CFR части 11 в редакции от 1 апреля 2015 г.

Подраздел B – электронные записи.

11.10. Контроль замкнутых систем.
Лица, которые используют замкнутые системы, чтобы создавать, изменять, сохранять или передавать электронные записи должны применять процедуры направленные на обеспечение подлинности, целостности, и, при необходимости, конфиденциальности электронных записей, и обеспечить, чтобы лица…. Такие процедуры и контроль должны включать в себя следующее:

1. Проверка системы, чтобы обеспечить точность, надежность, постоянство, предполагаемую производительность и способность различать недействительные или измененные записи.
   Сертификаты о внесении системы в Государственный Реестр Средств измерений подтверждает заявленную точность и воспроизводимость результатов измерений. В программной части системы отсутствует любая возможность изменять данные измерений.

2. Способность генерировать точные и полные копии записей как в человекочитаемой форме, так и в электронной форме, подходящей для осмотра, рассмотрения, и копирования проверяющим органом. Персоналу следует обратиться в агентство, если есть какие-либо вопросы, касающиеся способности агентства для выполнения такой обзор и копирование электронных записей.
   Архивы измерений доступны для просмотра, экспорта на бумажный носитель в человекочитаемой форме.

3. Защита записей, чтобы обеспечить их точность и быстроту извлечения в течение всего периода хранения записей.
   Записи измерений хранятся в базе данных, которая обеспечивает быстрый доступ к записям через программу под определенной пользователем/ролью.

4. Ограничить доступ к системе только авторизированному персоналу.
   Доступ в программу возможен только тем сотрудникам, у кого имеется непросроченная пара логин/пароль.

5. Использовать безопасные, сгенерированные компьютером метки времени аудита записи действий оператора, таких как операции изменения или удаления электронных записей. Записи аудита не должны перекрывать предыдущие записи. Такие записи аудита должны сохранятся на период, необходимый для анализа и должны быть доступны для проверяющих служб.
   Любые действия персонала в системе логируются. Удаление/модификация записей из системы невозможно. В данный момент информация записывается в текстовые лог файлы, время жизни которых обычно измеряется неделями. Возможно настроить автоматическое копирование лог файлов в защищенное хранилище. Также можно завести отдельную таблицу для записи аудита действий, что вообще предотвратит доступ неавторизированного персонала к этим данным.

6. Использование проверок операционной системы для обеспечения последовательности допустимых шагов и мероприятий, в соответствующих случаях.
   Действия пользователя логируются на уровне операционной системы. Доступ в операционную систему возможен только по логину/паролю.
7. Использовать проверки руководством, чтобы удостовериться что только авторизированный персонал может использовать систему, электронно подписывать записи, получать доступ к компьютерной системе и устройствам ввода-вывода информации, изменению записей и осуществления ручных операций.
   Доступ пользоваталей к системе регламентируется руководящем персоналом предприятия.

8. Использовать устройство или терминал для проверки в случае необходимости валидность источника данных для записей или операционных инструкций.
   Сертификаты Госреестра на измерительное оборудование подтверждают валидность измеренных данных.

9. Определить, что лица, которые разрабатывают, обслуживают или используют электронные записи имеют образование, подготовку и опыт для выполнения возложенных на них задач.
   Руководящий персонал предприятия допускает к использованию системы только определенных сотрудников, прошедших подготовку.

10. Основания и приверженность предписаниям, политикам, которые призывают физических лиц к ответственности и ответственности за действия, инициированные в рамках своих электронных подписей, для того, чтобы предотвратить электронные записи и цифровые подпись от фальсификации.
    Регламентируется руководящим персоналом предприятия.

11. Использовать соответствующее управление системной документацией, включая:
    1) Надлежащий контроль над распространением, доступом, использованием документации по работе с системой и обслуживанием.
    2) Пересмотр и изменение процедуры контроля для поддержания аудита, что документы о разработке и модификации системы упорядочены во времени.
    Производится управление системной документацией, упорядоченной по времени. Сюда же включается документацию о поверке и техническому обслуживанию системы.

11.30. Контроль открытых систем.
Лица, которые используют открытые системы, чтобы создавать, изменять, сохранять или передавать электронные документы должны применять процедуры управления, предназначенные для обеспечения подлинности, целостности, и, при необходимости, конфиденциальности электронных документов с точки их создания до точки их получения. Такие процедуры и контроль должны включать в себя те, которые определены в 11.10, в соответствующих случаях, и дополнительные меры, такие как шифрование документа и использования соответствующих стандартов цифровой подписи для обеспечения, в случае необходимости при обстоятельствах, запись подлинности, целостности и конфиденциальности.
Для вашего случая не актуально, так как используется закрытая система.

11.50. Определение подписи.
(a) Подписанные электронные записи должны содержать информацию о подписанте, которая четко показывает следующие вещи:
(1) Напечатанное имя подписанта.

(2) Дату и время создания подписи и
(3) Смысл (например, обзора, утверждения, ответственности, или авторства), связанных с подписью.
Каждая запись в системе об измерении сопровождается информацией о ее поступлении в систему, включая время и дату. При распечатке и экспорте данных присутствует информация о текущем пользователе системы.

(b) Вещи, обозначенные в параграфах (a) (1), (a) (2), (a) (3) этого раздела должны быть предметом контроля как электронные записи и должны быть частью любой человекочитаемой формой электронной записи (такой как электронный дисплей или распечатка).
При распечатке и экспорте данных присутствует информация о текущем пользователе системы а также дата и время.

11.70. Связывание записей и подписей.
Электронные подписи и подписи, выполненные от руки к электронным записям должны быть связаны с соответствующими электронными документами, чтобы обеспечить, что подписи не могут быть удалены, скопированы или иным образом переданы, чтобы фальсифицировать электронную запись с помощью обычных средств.

11.100. Основные требования.

(a) Каждая электронная подпись должна быть уникальна для каждого человека и не должна переприсваиваться или быть использована кем-то другим.
Каждый пользователь работает исключительно под своей учетной записью в системе.

(b) Перед тем как организация выпустит, присвоит, сертифицирует или произведет какие-либо еще действия с электронной подписью сотрудника необходимо удостовериться в личности сотрудника.
При выдаче пары логин пароль пользователю системы руководящий персонал компании удостоверяется кому выдается доступ в систему согласно штатного расписания.

(c) Люди, использующие электронные подписи, до или во время такого использования, должны удостоверится в агентстве, что электронные подписи в их системе, используемой на или после 20 августа 1997, предназначены, чтобы быть юридическим эквивалентом традиционных рукописных подписей.
(1) Сертификация должна быть представлена в бумажной форме и подписана с традиционной рукописной подписью, в Офис Региональных Операций (HFC-100), 5600 Фишерс-Лейн, Роквилль, Мэриленд 20857.
(2) Люди, использующие электронные подписи, по запросу агентства, должны обеспечить дополнительную сертификацию или свидетельство, что определенная электронная подпись - юридически обязательный эквивалент рукописной подписи подписывающего лица.

11.200. Элементы электронных подписей и управление ими.

- Электронные подписи, которые основаны не на биометрических данных должны:
(1) Используйте по крайней мере два отличных идентификационных компонента, такие как идентификационный код и пароль.
Выдается администратором системы мониторинга.

(i) Когда человек выполнит ряд подписаний во время единственного, непрерывного периода системного доступа, которым управляют, первое подписание должно быть выполнено, используя все компоненты электронной подписи; последующие подписания должны быть выполнены, используя по крайней мере один компонент электронной подписи, который может быть использован только сотрудником
(ii) Когда человек выполнит одно или более подписаний, не выполненных во время единственного, непрерывного периода системного доступа, которым управляют, каждое подписание должно быть выполнено, используя все компоненты электронной подписи.
(2) Должно быть использовано только истинным владельцем и:
(3) Должно быть проверено и исполнено, чтобы гарантировать, что предпринятое использование электронной подписи человека любым кроме ее подлинного владельца требует сотрудничества двух или больше человек.
Все действия в системе выполняются только под действительным пользователем, который входит в систему под своим логином и паролем, выданным администратором системы.

- Электронные подписи, основанные на биометрии, должны быть разработаны, чтобы гарантировать, что они не могут использоваться никем кроме их подлинных владельцев.

11.300. Управление идентификацией коды/пароли.

Люди, которые используют электронные подписи, основанные на использовании идентификационных кодов в сочетании с паролями, должны использовать средства управления, чтобы гарантировать их безопасность и целостность. Такие средства управления должны включать:

(a) Поддержку уникальности каждого объединенного идентификационного кода и пароля, такого, что ни у каких двух человек нет той же самой комбинации идентификационного кода и пароля.
На уровне программного обеспечения отсутствует возможность заведения в системе двух пользователей с одинаковыми учетными записями. Рекомендуется не хранить пароль в базе конфигурации Rapid SCADA, а использовать интеграцию с Active Directory.

(b) Обеспечить, чтобы идентификационные коды и выпуски пароля периодически проверялись, отзывались или пересматривались (например, чтобы покрыть такие события как устаревание пароля).
Система напоминает пользователям о необходимости смены пароля. Также об этом может напомнить сотрудникам администратор системы.

(c) Следующие процедуры по потере управления, когда теряется доступ к системе в электронном виде, когда доступ утерян, украден или иначе потенциально поставившие под угрозу карты и другие устройства, которые имеют или производят идентификационный код или информацию о пароле, и выпустить временные или постоянные замены, используя подходящие, строгие средства управления.
Существует механизм блокировки пользователей при потере реквизитов доступа, для предотвращения компрометации системы.

(d) Использование транзакций, чтобы предотвратить несанкционированное использование паролей и/или идентификационных кодов, и обнаружить и сообщить непосредственным владельцам и срочным способом о любых попытках их несанкционированного использования системы соответствующему менеджерскому персоналу.
На уровне программного обеспечения и операционной системы ведется журнал действий пользователя, в том числе о попытках несанкционированного доступа.

Неудачные попытки входа в настоящее время фиксируются в логах. Если необходимо, можно реализовать нотификацию системного администратора в этих случаях.

(e) Начальное и периодическое тестирование устройств, таких как токены или карты, которые несут или генерируют идентификационный код или информацию о пароле, чтобы гарантировать, чтобы они функционировали должным образом и не были изменены несанкционированным способом.

Рекомендуется использование стороннего программного продукта «Keepass» для хранения информации о пользователях и генерации новых паролей. Продукт бесплатен и предлагает самые стойкие алгоритмы шифрования.