Synergy

Przewodnik po walidacji

automatyka i pomiary

Hanwell Synergy
Oprogramowanie Synergy i wymagania FDA 21 CFR Part 11

Przedsiębiorstwo Automatyzacji i Pomiarów Introl Sp. z o.o.
40-519 Katowice, ul. Kościuszki 112
tel. +48 32 789 01 30, fax +48 32 789 00 10
e-mail: temperatury@introl.pl

Wydanie luty 2015

Spis treści

1. Historia

Rewizja	Data	Szczegóły rewizji
1	27/01/2014	Utworzenie dokumentu

2. Wprowadzenie

FDA 21CFR Part 11 są to przepisy FDA (Agencja ds. Żywności i Leków USA) dotyczące bezpieczeństwa zapisu danych elektronicznych. Dotyczy to również podpisu elektronicznego na zapisie.
Oprogramowanie Synergy, zarówno dla systemów zdalnego monitoringu jak i dla samodzielnych rejestratorów danych, może być dostarczane z zezwoleniem Control Licence FDA 21CFR Part11 oraz dokumentami potwierdzającymi testy IQ i OQ (kwalifikacja instalacyjna i operacyjna) obejmujące cechy wymagane dla spełnienia zgodności z wymaganiami przepisów FDA 21CFR Part11. Zapewnia to, że zapisy elektroniczne – czy to w formie rekordów danych, czy w formie **rejestru zdarzeń / dziennika audytu** – nie mogą być zmienione, a każda próba ingerowania w nie będzie odnotowana.

2.1 Założenia

Nie jest to możliwe, aby jakakolwiek aplikacja zapewniała wewnętrznie pełną zgodność z wymaganiami FDA 21CFR Part11, jeśli ta aplikacja nie kontroluje całkowicie komputera PC. Ponieważ taka kontrola normalnie nie jest dozwolona w systemach informatycznych sieci korporacyjnych, to zakładamy, że reżim bezpieczeństwa danego systemu operacyjnego został zaplanowany i wdrożony przez dział IT danej korporacji. Działanie takie musi zabezpieczać przed nieupoważnionym dostępem do bazy danych i kasowaniem lub zmianą nazwy plików.
Zakładamy również, że dostęp do funkcji kontrolujących dostęp do oprogramowania **Synergy** będzie ściśle ograniczony i tylko możliwy dla administratora Synergy: zalecamy, aby ilość administratorów systemu była ograniczona.

2.2 Trzy kroki do zgodności

Walidowane oprogramowanie Synergy jest tak skonstruowane, aby umożliwić proste, krok po kroku postępowanie w celu uzyskania zgodnego walidowanego systemu. Standardowe oprogramowanie Synergy Pharmaceutical lub Health care może być zainstalowane i używane jako niekwalifikowany system, a gdy okoliczności tego wymagają, to standardowy system może być przeniesiony w kilku łatwych krokach do poziomu kwalifikowanego systemu.

Oprogramowanie Synergy jest dostarczane z protokołami kwalifikacji instalacji IQ, które muszą być wypełnione w momencie instalowania oprogramowania. Kody zamówienia oprogramowania są następujące:

- W706A dla instalacji wymagających zainstalowania SQL na lokalnym komputerze.
- W706B dla instalacji wymagających zainstalowanego SQL.

Poniższe kroki można wykonać w dowolnym momencie jednorazowo lub mogą być zastosowane w czasie, według wymagań.

1. Aby odblokować cechy wymagane do uzyskania systemu zgodnego z wymaganiami 21 CFR Part 11, należy użyć licencji walidowanego oprogramowania Synergy. Numer części z licencją to W701.
2. Dzienniki robocze OQ oprogramowania wstępnie skompletowane przez inżynierów IMC mają numer części W707. W707 obejmuje wszystkie funkcje oprogramowania, na które nie ma wpływu środowisko instalacji. Dzienniki robocze OQ oprogramowania dostarczane są w formie drukowanych segregatorów z 4 pierścieniami.
3. Szablony sprzętowe IQ i OQ oraz szablony IQ dla oprogramowania są dostępne do sfinalizowania na miejscu przez personel IMC, przez autoryzowanych przez IMC dystrybutorów lub przez działy jakości Użytkowników. Szablony dostarczane są w formie drukowanych segregatorów z 4 pierścieniami. Dostępne są również kopie elektroniczne.

3. Wymagania FDA 21CFR Part 11

W niniejszym punkcie opisane są szczegółowo wymagania FDA 21CFR Part 11 oraz sposób w jaki realizuje je oprogramowanie Synergy Validated. Firma Hanwell zaleca wszystkim administratorom systemów zgodnych z Part 11 przeczytać definicję FDA 21CFR Part11. Aby skonfigurować Synergy jako system walidowany, użytkownik musi zakupić i aktywować licencję walidującą W701 i zrealizować wymagane protokoły walidacji, które spowodują odblokowanie cech wymaganych do uzyskania zgodności.

3.1 Podpisy elektroniczne

Przepisy 21CFR Part 11 stwierdzają, że dostęp do aplikacji może być uzyskany tylko poprzez dwa identyfikatory: **Nazwa i Hasło użytkownika**, i że kombinację tych dwóch identyfikatorów może znać tylko użytkownik. Każde działanie użytkownika, które jest zapisywane w dzienniku zdarzeń, dzienniku kontroli wymaga, że działanie to musi być sprawdzone poprzez wprowadzenie **Hasła użytkownika** przed zrealizowaniem tego działania.
W oprogramowaniu będzie działała funkcja umożliwiająca każdemu użytkownikowi działać jako kontrasygnator lub zatwierdzający działania wykonywane przez administratorów systemu takie, jak zmiany dokonywane w dziale Admin.

3.2 Zgodność podpisu elektronicznego

Administrator systemu utworzy Nazwę Użytkownika i ustawia standardowe hasło, które będzie użyte do zalogowania się po raz pierwszy. Szczegóły użytkownika będą obejmowały jego pełne nazwisko. W tym czasie są również ustawiane prawa dostępu i przywileje dotyczące przeglądania. Gdy nowy użytkownik loguje się po raz pierwszy, to będzie zmuszony zmienić swoje hasło, które od tego momentu będzie znane tylko jemu. Nazwa Użytkownika będzie używana do zidentyfikowania wszystkich istotnych działań wykonywanych przez tego użytkownika.

3.2.1 Zabezpieczenia hasła użytkownika

Ten punkt dotyczy tylko haseł użytkownika oprogramowania Synergy Validated, nie dotyczy logowania się do systemów poczty elektronicznej lub SQL, które będą znajdowały się pod kontrolą administratora systemu IT użytkowników. Ze środowiska operacyjnego oprogramowania Synergy nie ma żadnego dostępu do SQL.
Standardowo Synergy wymaga haseł o długości co najmniej 8 znaków, czyli Administrator nie będzie mógł ustawić minimalnej długości hasła mniejszej niż 8 znaków. Jest to konfigurowane przez Administratora. ID i hasło użytkownika nie mogą być takie same.
Administrator może również wymagać, żeby hasła użytkowników składały się z dużych i małych znaków alfanumerycznych.

3.2.2 Wygaśnięcie hasła

Standardowo hasła użytkowników tracą ważność w ciągu 90 dni, czas ten jest ustawiany przez administratora.
Użytkownik podczas logowania się będzie ostrzegany na 10 dni przed datą wygaśnięcia hasła i udostępniona jemu będzie opcja wprowadzenia nowego hasła w dowolnym czasie między pierwszym ostrzeżeniem i datą wygaśnięcia. Czas ostrzegania będzie ustawiany przez administratora. Będzie to ostrzeganie z odliczaniem w dół i wartość odliczana będzie zmniejszać się wraz ze zbliżaniem się terminu wygaśnięcia.
Jeśli ważność hasła wygasła, to użytkownik będzie miał zablokowany dostęp do momentu, aż wprowadzi hasło, którego ważność wygasła, i w tym momencie system wymusi zmianę hasła zanim użytkownik będzie mógł wykonywać jakiekolwiek działania.
Głębokość hasła może być ustawiona globalnie między 1 i 10. Parametr głębokość hasła ustawia liczbę poprzednich haseł, których użytkownik nie może natychmiast użyć ponownie.

3.2.3 Nieudane próby wprowadzenia hasła i zablokowanie dostępu

Standardowo dostęp użytkownika zostanie zablokowany przez 60 minut po 3 kolejnych nieudanych próbach zalogowania się w czasie 30 minut. Gdy dojdzie do zablokowania dostępu, użytkownik zostanie poinformowany o okresie zablokowania za pomocą komunikatu na przeglądarce, a zablokowanie zostanie zapisane w dzienniku działań.
Blokada dostępu o wartości 0 zablokuje użytkowników aż do momentu resetu przez Administratora. Każde zablokowanie samego administratora będzie trwać 30 minut (zapobiega to możliwości trwałego zablokowania Administratora).
Pole wyboru Reset Lockout (Reset blokady) jest dostępne na ekranie User Details (Szczegóły użytkownika). To pole jest normalnie szare i staje się aktywne tylko wtedy, gdy użytkownik ma zablokowany dostęp. Pole to jest dostępne tylko dla administratora.

3.2.4 Nazwa użytkownika

Każdemu użytkownikowi będzie przypisane ID użytkownika i pełna nazwa, która będzie imieniem i nazwiskiem użytkownika, a ID użytkownika będzie skróconą formą nazwiska, za pomocą której użytkownik będzie logował się do systemu.
ID i pełna nazwa użytkownika muszą być niepowtarzalne i będą sprawdzane.
Gdy użytkownik zostanie wykluczony z systemu, to jego nazwa użytkownika nie może być nigdy powtórnie użyta
Jeśli Administrator spróbuje wprowadzić poprzednio używaną nazwę użytkownika na ekranie User Details, to wyświetli się komunikat ostrzeżenia mówiący, że ta nazwa była już używana i nie jest dostępna. Administrator może otrzymać raport podający listę aktualnych i byłych użytkowników, obejmujący:

- Status użytkownika (aktywny lub wykluczony)
- Datę dodania użytkownika
- ID użytkownika
- Imię i nazwisko
- Datę wykluczenia użytkownika

3.2.5 Automatyczne wylogowanie

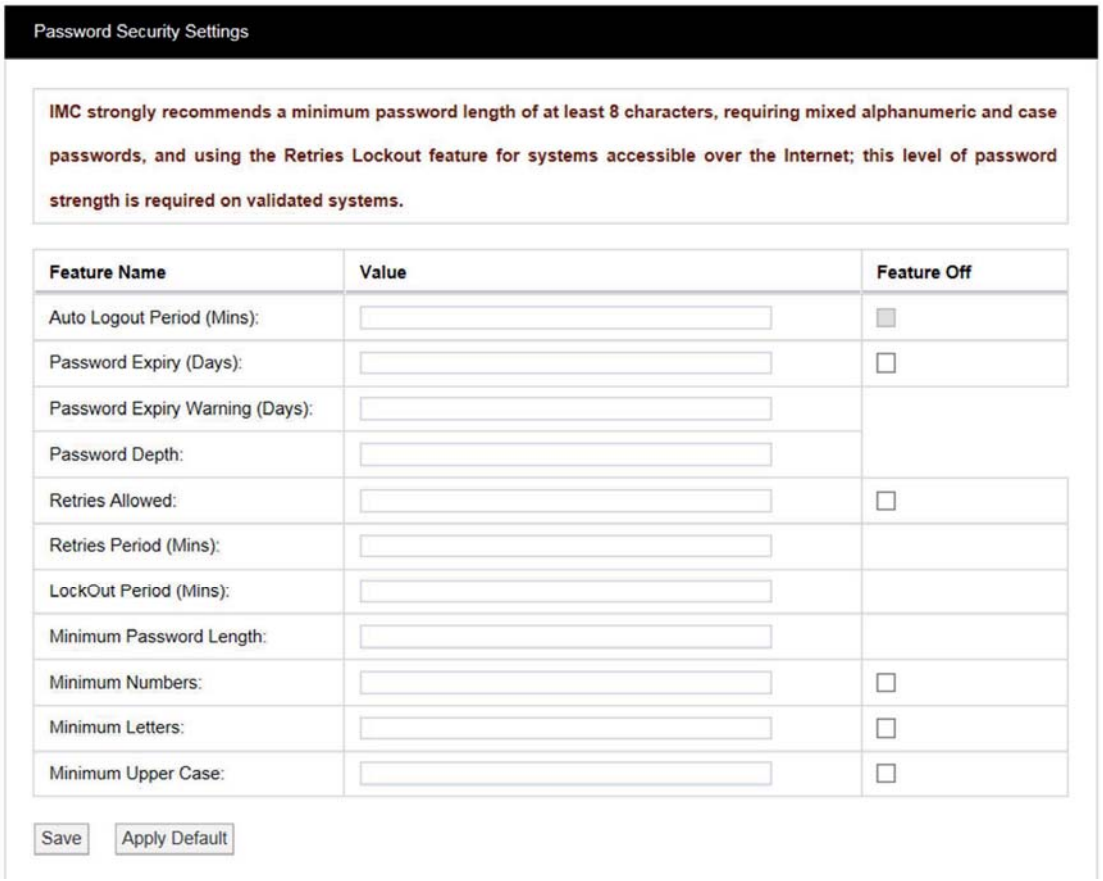
Czas automatycznego wylogowania jest ustawiany przez Administratora. Standardowe ustawienie wynosi 15 minut. Jeżeli w ustawionym czasie automatycznego wylogowania użytkownik nie wykonuje żadnych działań, to zostanie automatycznie wylogowany.
Funkcji automatycznego wylogowania nie można wyłączyć.

3.2.6 Utrata hasła

Jeżeli użytkownik zapomni swoje hasło dostępu, to będzie musiał skontaktować się z administratorem, który skasuje hasło. Użytkownik, który zapomniał hasło będzie musiał zamienić swoje hasło zanim będzie mógł kontynuować pracę w systemie.
Gdy zostanie zastosowana procedura kasowania hasła, to zostanie to zapisane w dzienniku zdarzeń/kontroli pod ID użytkownika.

3.2.7 Ustawianie zabezpieczeń hasła

Ekran ustawiania zabezpieczeń hasła użytkownika jest dostępny poprzez zakładkę Password Security Settings (Ustawienia zabezpieczenia hasła) na menu po lewej stronie ekranu User Management (Zarządzanie Użytkownikami).



3.2.8 Akceptowany zakres wartości

Poniżej podane są zakresy ustawień dla każdej opcji:

- Auto Logout (Automatyczne wylogowanie) – 5 do 60 minut.
- Password Expiry (Czas wygaśnięcia hasła) – 30 do 730 dni.
- Password Expiry Warning (Ostrzeżenie o wygaśnięciu hasła) – 1 do 10 dni.
- Password depth (Głębokość hasła) – 1 do 10.
- Retries Allowed (Ilość prób wprowadzenia hasła) – 1 do 10 prób.
- Lockout Period (Czas trwania zablokowania) – 0 do 1440 minut; 0 blokuje użytkowników aż do resetu przez Administratora.
- Retries Period (Czas próbowania wprowadzenia hasła) – 10 do 1440 minut.
- Minimum Password Length (Minimalna długość hasła) – 8 do 50 znaków.
- Minimum Numbers, Minimum Letters, i Minimum Upper Case (Minimalna ilość cyfr, liter i dużych znaków) – 1 do 50, wartości te są sprawdzane pod względem minimalnej długości i liczby.

3.2.9 Wydruk i podpisywanie raportu

Każdy z raportów i wykresów będzie zawierał poniższe szczegóły dodane do wydruku na każdej stronie:

- Tytuł dokumentu
- ID użytkownika
- Znacznik daty i czasu
- Rubryka z nazwiskiem i podpisem użytkownika oznaczona „Sporządził”
- Rubryka z nazwiskiem i podpisem sprawdzającego oznaczona „Zatwierdził”
- Rubryka do wpisania przez użytkownika powodu utworzenia raportu/wydruku oznaczona „Komentarze”

Każde działanie użytkownika, które dołącza jego ID do raportu lub wydruku będzie wymagać wprowadzenia hasła użytkownika przed zrealizowaniem tego działania.

3.3 Ochrona integralności danych

W walidowanych systemach integralność magazynowanych danych, alarmów i dzienników kontrolnych jest chroniona przed ingerowaniem w struktury danych i te zabezpieczenia będą zaimplementowane tylko wtedy, gdy zostanie zastosowana licencja walidowanego systemu. Przy jakiejkolwiek próbie modyfikacji pola chronionych danych, zmiana zostanie odrzucona, dane zalogowania zostaną zapisane w Dzienniku działań (Activity Log) i szczegóły dotyczące próby modyfikacji zostaną wysłane mailem do administratora.

Dla dodatkowego zabezpieczenia powyższa procedura nie jest zewnętrznie dokumentowana, lecz jest całkowicie sprawdzalna. W ramach środowiska operacyjnego użytkownika Synergy nie istnieje żaden mechanizm umożliwiający zmianę lub usunięcie

danych.

3.4 Poziomy dostępu

Dostęp do funkcji oprogramowania Synergy jest ograniczony w zależności od poziomu prawa dostępu przyznanego nazwie użytkownika przez Administratora systemu. Jeżeli użytkownik próbuje przejść do funkcji, do której nie ma prawa dostępu, to otrzyma odmowę dostępu i komunikat „Odmowa dostępu. Nie masz uprawnień do wykonywania tego zadania, skontaktuj się z Administratorem systemu". To ustawienie nie może być zmienione przez Użytkowników.
W oprogramowaniu Synergy nie ma z góry zdefiniowanych poziomów dostępu. Klient może swobodnie określać poziomy dostępu dla swoich użytkowników. Funkcja kontroli dostępu w Synergy służy do utworzenia Grup Uprawnień użytkownika, gdzie do każdej grupy przydzielone są różne prawa, a użytkownicy dodani do danej Grupy nabywają uprawnienia przydzielone do tej Grupy. Można dodawać dowolną ilość poziomów w zależności od potrzeb.
Poniżej przedstawione są sugerowane Grupy Uprawnień:

- Pełny administrator
  Jest to główny **Administrator systemu**: Administrator systemu ma dostęp do wszystkich funkcji i odpowiada za przydzielanie **nazwy użytkownika, prawa dostępu i przywilejów przeglądania**. Normalnie w systemie istnieje tylko 1 lub 2 pełnych administratorów.
- Administrator ogólny
  Administrator ogólny systemu na ogół nie ma uprawnień do przydzielania lub zmieniania **nazwy użytkownika, prawa dostępu i przywilejów przeglądania**. Na tym poziomie użytkownik może dodawać i usuwać czujniki, ustawiać poziomy alarmu i edytować funkcje Email & SMS- alarmów, etc.
- Użytkownik zaawansowany
  Na tym poziomie użytkownik może potwierdzać alarmy, generować raporty o wyjątkowych sytuacjach, etc. i może edytować ustawienia systemu lub ustawienia Email & SMS- alarmów.
- Użytkownik standardowy
  Na tym poziomie użytkownik może potwierdzać alarmy, generować raporty o wyjątkowych sytuacjach, etc., lecz nie może edytować ustawień systemu lub ustawień Email & SMS- alarmów.
- Użytkownik gość
  Na tym poziomie użytkownik może przeglądać aktualne dane i wykresy, lecz nie może potwierdzać alarmów lub zmieniać sposobu przedstawiania wykresów.

Powyższe jest tylko sugestią i jest całkowicie konfigurowalne przez klienta.

4. Metodologia walidowania dokumentacji

GAMP 5 umożliwia pragmatyczne, oparte na analizie ryzyka podejście do walidacji skomputeryzowanych systemów. Na podstawie GAMP5 oprogramowanie Synergy jest sklasyfikowane jako **system zamknięty kategorii 4**.

W niniejszym punkcie jest przedstawione nasze podejście do dokumentacji walidacyjnej dla Synergy Validated. Dokumentacja walidacyjna oprogramowania Synergy jest podzielona na dwie części zawierające **Dokumenty Kwalifikacyjne Oprogramowania** i **Dokumenty Kwalifikacyjne kwalifikacji instalacyjnej i operacyjnej IQ/OQ oprogramowania i sprzętu**.
Dokumenty kwalifikacyjne oprogramowania testują i walidują stałe części programu, które nie zmieniają się w zależności od instalowania lub nie podlegają wpływom środowiska instalacji. GAMP5 sugeruje, że użytkownik systemu powinien mieć wpływ na każdą dokumentację wytwarzaną przez projektantów systemu, i takie dokumenty będą tworzone orazi kompletowane przez zespół inżynierów IMC oraz udostępnione do zakupu.
Przy każdej modyfikacji oprogramowania Synergy będzie aktualizowana **dokumentacja kwalifikacyjna oprogramowania** jak to jest wymagane, będzie przerobiona, podpisana i zapisana z najnowszą wersją. Poprzednia wersja zostanie zarchiwizowana i przechowywana z jej wersją oprogramowania.
Dokumenty Kwalifikacyjne kwalifikacji instalacyjnej i operacyjnej IQ/OQ oprogramowania i sprzętu będą zawierać wzorce IQ & OQ do walidacji aktualnej instalacji i części oprogramowania konfigurowalnych przez użytkownika.
Przy każdej aktualizacji oprogramowania Synergy zostaną również zaktualizowane **Dokumenty Kwalifikacyjne kwalifikacji instalacyjnej i operacyjnej IQ/OQ oprogramowania i sprzętu**. Poprzednia wersja zostanie zarchiwizowana i przechowywana z jej wersją oprogramowania.
Kompletny zestaw dokumentów walidacyjnych Synergy zostanie sporządzony zgodnie z GDP/GDocP (praktyka dobrej dokumentacji).

4.1 Dokumenty kwalifikacyjne oprogramowania

Dokumenty kwalifikacyjne oprogramowania będą zawierać kilka dokumentów, z których każdy będzie dotyczył części oprogramowania, co jest szczegółowo przedstawione poniżej.

4.1.1 Zarządzanie użytkownikiem

Dokumentacja zarządzania użytkownikiem obejmuje:

- Adding Users
- Deleting Users
- Editing Users
- Creating External Contacts
- Creating User Groups
- Deleting User Groups
- Editing User Groups
- Setting User Group Privileges
- Removing User Group Privileges
- Permissions Overview
- Manage Roles
- Role Definitions
- Manage Users
- Manage Permissions

4.1.2 Bezpieczeństwo systemu

Dokumentacja bezpieczeństwa systemu obejmuje:

- Password control
- Unauthorised access attempt control
- Data integrity

4.1.3 Konfiguracja pod-systemów alarmów

Dokumentacja konfiguracji systemu obejmuje:

- Email Alert Global Settings
- SMS Alert Global Settings
- Email Heartbeat Group
- SMS Heartbeat Group
- Email System Group
- SMS System Group
- Synergy and FDA 21 CFR Part 11
- Doc No. SV-5296 Page 10 of 12

4.1.4 Grupowanie czujników

Dokumentacja miejsc obejmuje:

- Tworzenie miejsc/stref
- Przeglądanie miejsc/stref
- Edytowanie miejsc/stref
- Dodawanie sub-miejsc
- Usuwanie miejsc/stref
- Przeglądanie sub-miejsc/stref
- Dodawanie miejsc/stref do pulpitu sterowania

4.1.5 Zarządzanie konfiguracją czujników

Dokumentacja konfiguracji systemu (czujniki) obejmuje:

- Adding Sensors
- Manual Input Sensors
- Copy Sensors
- Delete Sensors
- Configuring Sensors
- Accessing Sensor Properties
- General Properties
- Calibration
- Alarms
- Global Settings
- Global Units

4.1.6 Konfiguracja urządzenia zbierającego

Dokumentacja konfiguracji urządzenia obejmuje:

- Setting up the Database Logger Service
- Edit/View DB Service
- Hardware Services
- Edit/View HW Services
- Add Devices
- Edit/View Devices
- Create Device Groups
- Edit/View Device Groups

4.1.7 Przeglądanie danych

Dokumentacja przeglądu danych obejmuje:

- Graphing Data
- Normal Conditions
- Alarm Condition indication
- Out of Service sensors
- Overlaying Sensors
- Range Alarms
- Level Alarms
- Reset
- Previous
- Next
- Display Modes
- Export Data
- Special Functions
- Graph Zoom
- Graph View Live Data
- View Data Graph Titles
- Viewing Bar Charts
- Viewing Data in Plan View
- Synergy and FDA 21 CFR Part 11
- Doc No. SV-5296 Page 11 of 12

4.1.8 Funkcjonalność alarmów

Dokumentacja zarządzania alarmami obejmuje:

- System Status Overview
- System Alarm Status Overview
- Communications Status
- Locating Alarms on the System
- Acknowledging Alarms
- Acknowledging Individual Alarms
- Acknowledging Multiple Alarms
- Email alarms functionality
- SMS alarms functionality

4.1.9 Dzienniki systemu

Dokumentacja dzienników systemu obejmuje:

- Activity Log
- Alarm Log
- SMS Log
- Email Log

4.2 Dokumenty kwalifikacyjne IQ/OQ oprogramowania i sprzętu

4.2.1 Konfiguracja oprogramowania

Dokumentacja konfiguracji oprogramowania obejmuje:

- Kwalifikacja instalacyjna IQ oprogramowania
- Kwalifikacja instalacyjna IQ konfiguracji systemu wg specyfikacji klienta, obejmująca
  - Czujniki
  - Grupowanie czujników
  - Przydział użytkownika
  - Ustawienie raportów
  - Ustawienia alarmów
  - Konfigurację zewnętrznych alarmów (e-mail i SMS wg potrzeb)
  - Ustawienie archiwizacji

4.2.2 IQ & OQ sprzętu

Dokumentacja kwalifikacyjna IQ & OQ sprzętu obejmuje fizyczny sprzęt systemu:

1. IQ &OQ SR2
2. IQ & OQ przetworników radiowych
3. IQ & OQ repeatorów
4. IQ & OQ modułu SMS AW04

4.2.3 Sprawdzenie w obwodzie zamkniętym

Niniejszy punkt obejmuje dostarczenie zindywidualizowanej dokumentacji umożliwiającej sprawdzenie w obwodzie zamkniętym następujących elementów:
Kwalifikacja operacyjna OQ poziomu alarmu z uruchomieniem alarmów za pomocą sztucznych czujników, kalibratorów procesu, bloków grzejnych, generatorów wilgoci, urządzeń do generowania ciśnienia lub gazów kalibracyjnych, etc.
Kwalifikacja operacyjna OQ kalibracji i dokładności czujnika za pomocą kalibratorów procesu, bloków grzejnych, generatorów wilgoci, urządzeń do generowania ciśnienia lub gazów kalibracyjnych, etc

5. Dokumenty wspomagające

Oprogramowanie Synergy Validation jest wspomagane następującymi dokumentami:

- Podręcznik instalacji.
- Podręcznik użytkownika.
- Specyfikacja użytkownika.
- Dokumentacja przeglądowa systemu.
- Schemat blokowy systemu.
- Certyfikaty szkolenia dystrybutorów / certyfikaty autoryzacji.

Przedsiębiorstwo
Automatyzacji i Pomiarów
Introl Sp. z o.o.

ul. Kościuszki 112
40-519 Katowice
tel: +48 32 789 00 00
fax: +48 32 789 00 10
internet: www.introl.pl
e-mail: introl@introl.pl