AKADEMIA MORSKA
W SZCZECINIE

WYDZIAŁ NAWIGACYJNY

LABORATORIUM SIECI I MOBILNYCH TECHNOLOGII PRZESYŁU DANYCH
(LSTPD)

Stanowisko 2 – MODBUS TCP/IP

Ćwiczenie I – prezentacja protokołu

Opracowali:
mgr inż. Bilewski Mateusz
mgr inż. Duczkowski Marek
dr inż. Gucma Maciej

1 Informacje wstępne *[Introduction]*

Opis protokołu Modbus TCP/IP

Stanowisko laboratoryjne nr 2 przedstawia jeden ze sposobów komunikacji przemysłowej sieci komputerowej jakim jest protokół Modbus TCP/IP. Modbus TCP/IP jest protokołem otwartym, opierającym się na TCP/IP. Protokół ten stał się standardowym rozwiązaniem dla przemysłowych interfejsów Ethernet. Modbus TCP/IP korzysta z portu 502. Dla wymiany danych procesowych, wymiany danych parametrów oraz identyfikacji urządzenia dostępne są następujące operacje FC (Function Codes).

- FC3 – Read Holding Registers,
- FC16 – Write Multiple Registers,
- FC23 – Read Write Multiple Registers,
- FC43 – MEI, Type 0x0E „Read device identification”.

Poprzez Modbus TCP/IP, urządzenie slave przedstawione jest jako złożony blok rejestru. Blok ten może zawierać do 64k słów i reaguje od numeru odniesienia (Offeset) 0. W tym bloku rejestru przechowywane są dane procesowe falownika oraz jeden kanał parametrów. Dla cyklicznej wymiany danych procesowych za pomocą Modbus – Master (Client), dostępne są operacje FC3, FC16 i FC23, przy czym zaleca się korzystanie z operacji FC23. Karta opcji DFE11B pozwala na wymianę do dziesięciu słów danych procesowych przy użyciu Modbus – Master (Client).

Rozwiązania komunikacyjne oparte o protokół TCP/IP błyskawicznie znajdują kolejne zastosowania obejmujące również jeden z bardziej zachowawczych obszarów wykorzystania technologii informatycznej, jaką jest dziedzina informatyki przemysłowej. W chwili obecnej stos protokołów TCP/IP wykorzystywany jest już nie tylko w sferze zdalnej prezentacji informacji opisującej proces technologiczny czy też w warstwie wizualizacji procesu realizowanej na poziomie stacji kontrolno-nadzorczej klasy SCADA, ale przechodząc przez poszczególne szczeble hierarchicznej struktury systemu informatyki przemysłowej, znajduje on zastosowanie na poziomie urządzeń zaangażowanych w sposób bezpośredni w kontrolę i sterowanie procesem przemysłowym.

Obecnie stosowane są dwa reprezentatywne mechanizmy komunikacyjne oparte o protokół TCP/IP, stosowane współcześnie dla węzłów systemu czasu rzeczywistego. Są to dwa podstawowe obszary zastosowania protokołu TCP/IP widziane przez pryzmat węzła systemu informatyki przemysłowej. Pierwszy z obszarów dotyczy zdalnej prezentacji informacji dostarczanej przez węzeł systemu w sieci Internet, drugi obszar obejmuje

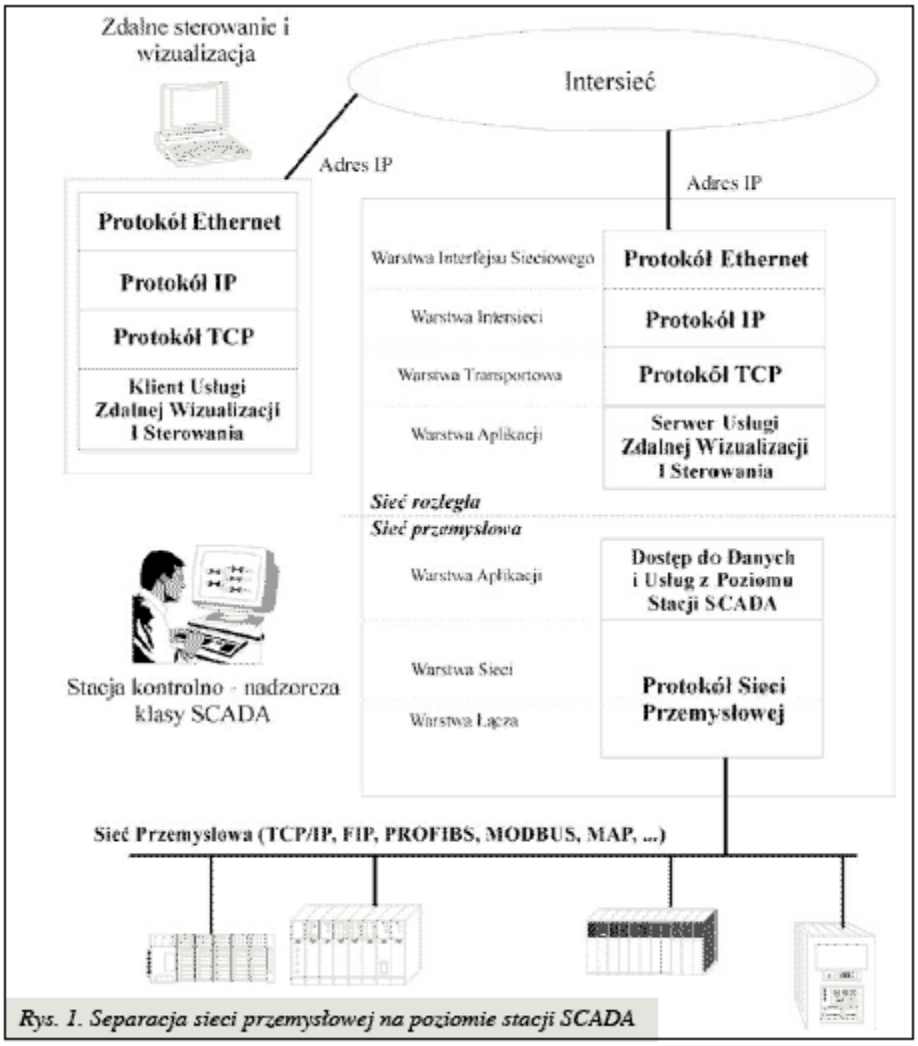
wymianę informacji pomiędzy węzłami sieci, z wykorzystaniem protokołów komunikacyjnych budowanych na bazie TCP/IP.

Przyczyn rosnącej popularności protokołu TCP/IP w rozwiązaniach automatyki przemysłowej należy upatrywać w dobrej standaryzacji tej rodziny protokołów, braku opłat licencyjnych związanych z ich wykorzystywaniem oraz w powszechnej dostępności rozwiązań sprzętowo-programowych niezbędnych do ich implementacji.

Z drugiej strony instalacje automatyki przemysłowej zaczynają tracić swoją pierwotną hermetyczność. Postępująca decentralizacja układów automatycznego sterowania sprawia, iż rozproszone systemy automatyki przemysłowej wymieniają coraz większe ilości danych nie tylko pomiędzy rozmieszczonymi na terenie obsługiwanej instalacji urządzeniami, ale również wymaga się od nich zapewnienia ciągłego kontaktu ze światem zewnętrznym. Potrzeba „otwarcia się na otaczający świat", stymulowana przez rozwijającą się dynamicznie e-gospodarkę sprawiła, iż od przemysłowych systemów sterowania wymaga się w coraz szerszym zakresie współpracy z sieciami rozległymi, w tym także coraz częściej z konstruowaną na bazie protokołu TCP/IP siecią Internet. Wymienione powyżej fakty sprawiają, iż we współcześnie tworzonych systemach automatyki przemysłowej protokół TCP stosowany jest coraz powszechniej, poczynając od poziomu wizualizacji zakładowej infrastruktury informatycznej, systemów sterowania i wizualizacji klasy SCADA, a na zdalnym dostępie do zasobów węzła systemu automatyki przemysłowej z poziomu sieci Internet kończąc.

Pierwotnie rozwiązania urządzeń konstruowanych do prezentacji danych procesowych przez sieć Internet oparte były o stosunkowo niedrogie układy zawierające dedykowane rozwiązania mikroprocesorowe, pozwalające na bezpośrednie sprzęgnięcie aparatury obiektowej z Intersiecią. Przykładem takiego urządzenia może być oferowany przez firmę Rabbit Semiconductor, układ oparty na procesorze Rabbit 3000. Bezpośredni sprzęg z obsługiwanym obiektem zapewniają elementy wejść/wyjść cyfrowych i analogowych, jak również obsługiwane przez procesor porty komunikacji szeregowej RS485. Obsługa protokołu komunikacyjnego dla łącza szeregowego realizowana jest w postaci procedury bibliotecznej obsługiwanej w podstawowej pętli mikroprocesora Rabbit. W pętli tej mikroprocesor obsługuje również interfejs sieci Ethernet, a dostarczone moduły biblioteczne zawierają implementację protokołów: TCP, UDP, ICMP, HTTP, SMTP, FTP, TFTP. Producent przewiduje możliwość sterowania urządzeniami wykonawczymi za pomocą interaktywnych stron www. Niestety rozwiązanie takie, ze względu na opisane powyżej łączenie wszystkich części programu we wspólnej pętli, wydaje się problematyczne dla zastosowania w systemach czasu rzeczywistego.

Alternatywą dla powyższego rozwiązania może być zastosowanie stacji kontrolno-nadzorczej klasy SCADA jako elementu pozwalającego na separację sieci przemysłowej najniższego poziomu od sieci rozległej na poziomie warstwy aplikacji (rys. 1).



Rys. 1. Separacja sieci przemysłowej na poziomie stacji SCADA

Rozwiązanie to umożliwia całkowitą izolację dwóch niezależnych obiegów informacji, obiegu wewnętrznej dystrybucji danych na poziomie sieci przemysłowej i niezsynchronizowanego z nim obiegu zewnętrznego zapewniającego zewnętrzny dostęp do informacji o procesie przemysłowym. Zastosowanie separacji przez urządzenie pośredniczące, jakim może być dedykowany układ typu firewall, lub też stacja kontrolno-nadzorcza, sprawia, iż jakikolwiek ruch przychodzący z sieci rozległej zostaje zatrzymany w warstwie aplikacji urządzenia pośredniczącego, decydującej o czasie i możliwości wykorzystania usług dostępnych w sieci przemysłowej najniższego poziomu. Odpowiednio skonstruowane oprogramowanie umożliwia realizację funkcji serwera usług, pozwalając na dostęp do zasobów znajdujących się po stronie sieci przemysłowej. Dodatkową zaletą takiego rozwiązania jest zwiększenie bezpieczeństwa systemu poprzez możliwość wprowadzenia szeregu mechanizmów kontroli dostępu, jak np. mechanizmów

uwierzytelniania i autentyfikacji oraz mechanizmów zapewniających poufność transmisji informacji poprzez sieć rozległą. Na tym poziomie możliwe jest zaimplementowanie mechanizmów bezpiecznych usług, jak np. mechanizmu szyfrowania z kluczem publicznym. Nie bez znaczenia pozostaje możliwość integracji różnego typu sieci przemysłowych z siecią rozległą. Opisywany model pozwala na połączenie przez sieć rozległą nie tylko urządzeń automatyki wyposażonych w interfejs komunikacyjny o protokole TCP/IP, ale również innych typów sieci przemysłowych. Możliwość taka staje się szczególnie istotna w kontekście dyskutowanych wcześniej zagadnień determinizmu czasowego.

Najpoważniejszą z punktu widzenia bezpieczeństwa wadą, związaną z wykorzystaniem urządzenia pośredniczącego pomiędzy systemem informatyki przemysłowej a siecią rozległą, jest jego podatność na atak z wykorzystaniem błędów systemu operacyjnego kontrolującego dostęp urządzenia. W takim przypadku atak na system operacyjny może spowodować nie tylko zaburzenie funkcjonowania stacji pośredniczącej, lecz także zakończyć się całkowitym upadkiem systemu informatyki przemysłowej oraz awarią współpracujących z nim układów automatyki.

Kolejną wadą rozwiązania opartego na powyższym modelu jest ograniczanie dostępu wyłącznie dla autoryzowanych użytkowników. Sytuacja taka sprawia, iż staje się niemożliwe wykorzystanie szeregu usług związanych z publicznym dostępem do danych, jak np. prezentacja wybranych informacji poprzez strony WWW.

Powyższe rozwiązanie niezbyt dobrze nadaje się do systemów, w których występuje większa liczba urządzeń pośredniczących, posiadających połączenie z siecią rozległą. W takim przypadku występowanie wielu punktów dostępu do sieci utrudnia jej skuteczną ochronę, a także wymaga tworzenia złożonych algorytmów rozstrzygających o prawach dostępu przez poszczególne urządzenia pośredniczące. Alternatywą dla urządzeń pośredniczących mogą być w tym przypadku rozwiązania oparte na portalach informacyjnych, w wydaniu przemysłowym.

Przemysłowe portale informacyjne umożliwiają spójną prezentację informacji pochodzących z różnych źródeł, takich jak: systemy wizualizacji klasy SCADA, systemy przemysłowych baz danych, systemy śledzenia produkcji, systemy gospodarki zasobami czy też systemy planowania i przygotowania produkcji. Pobierana z poziomu przemysłowej bazy danych informacja, udostępniana jest użytkownikowi po przeprowadzeniu filtracji i selekcji danych wewnątrz portalu. Do zadań portalu należy także: realizacja funkcji związanych z zapewnieniem bezpiecznego dostępu i autoryzacją użytkowników. Ze względu na znaczną skalę złożoności rozwiązania te realizowane są

zazwyczaj na poziomie całego przedsiębiorstwa, operując wielokrotnie na ogromnej ilości danych bieżących i danych archiwalnych. Przykładem rozwiązania wspierającego realizację przemysłowego portalu intranetowego może być pakiet SuiteVoyager firmy WonderWare.

2 Opis stanowiska *[Description of laboratory station]*

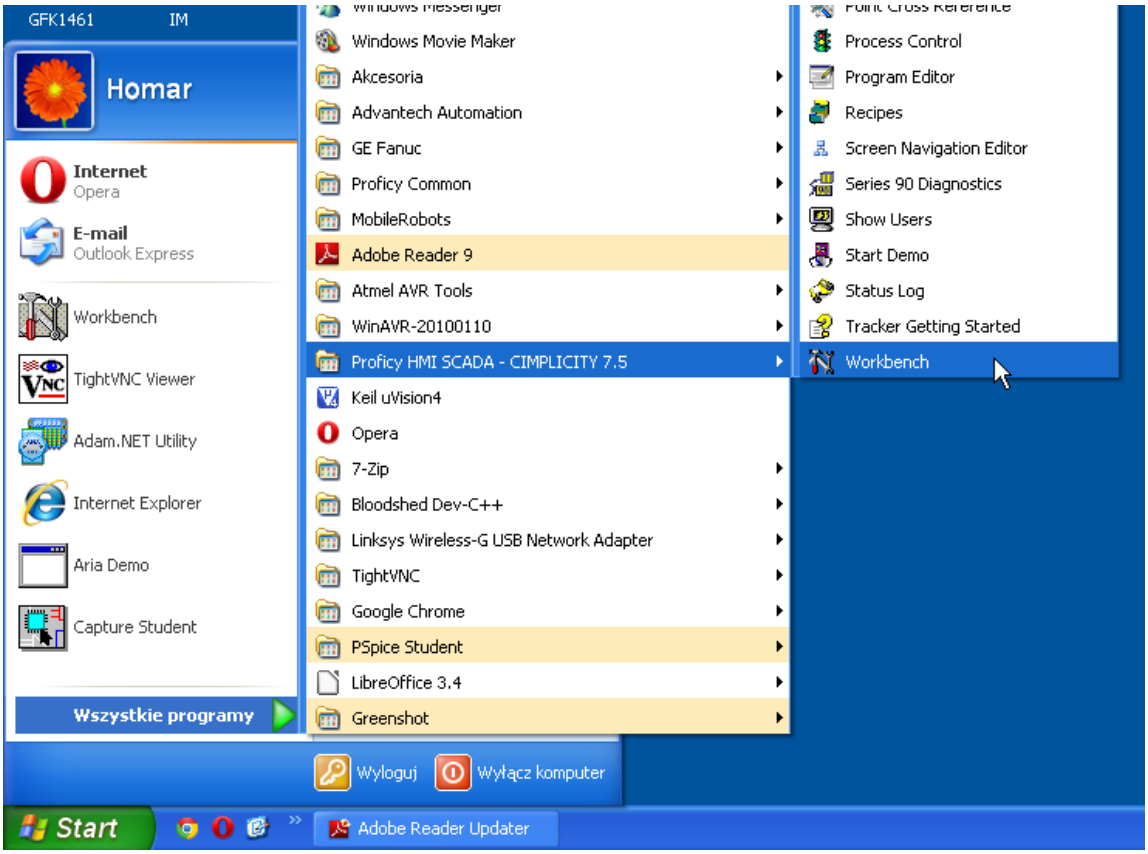
W skład stanowiska laboratoryjnego wchodzą: jedno urządzenie nadrzędne (Master - Wizualizacja HMI Proficy CIMPLICITY zainstalowana na komputerze PC), dwa urządzenia podrzędne (Slaves - Moduły I/O ADAM), oraz Switch ethernetowy niezbędny dla komunikacji urządzeń w standardzie TCP/IP, ponieważ element Master został zrealizowany na komputerze PC, wyposażonym w kartę sieciową z interfejsem RJ45.

- Modbus Master wykonany na komputerze, HMI Proficy CIMPLICITY - konfigurowany przez użytkownika, umożliwiający sterowanie jednostkami podrzędnymi typu Slave. Konfiguracja, oraz wizualizacja procesu komunikacji typu Modbus TCP/IP odbywa się z poziomu oprogramowania HMI.
- Moduły Modbus Slaves - konfigurowane przez użytkownika, sterowane zdalnie przy pomocy poleceń z jednostki Modbus Master. Moduły I/O typu ADAM posiadają unikalny adres w sieciowy komunikacji Modbus TCP/IP. Do komunikacji wykorzystane zostały następujące rodzaje modułów:
  - Moduł M6 ADAM 6050 – Moduł 12 wejść/6 wyjść dyskretnych.
  - Moduł M7 ADAM 6017 – Moduł 8 wejść analogowych.
  - Switch SW2 LINKSYS – Switch pozwala na pracę modułów w sieci o topologii gwiazdy. Switch podłączony jest do karty sieciowej komputera PC i załącza się w sposób automatyczny po jego zasileniu napięciem 12VDC.

Wszystkie moduły zasilone są napięciem stałym 24VDC z zasilacza obiektowego U4 znajdującego się z tyłu panelu sterowania. Zasilacz zabezpieczony jest wyłącznikiem nadmiarowo-prądowym F2 (nad prądowym) CLS6 C6/2 umieszczonym również na tylnej szynie.

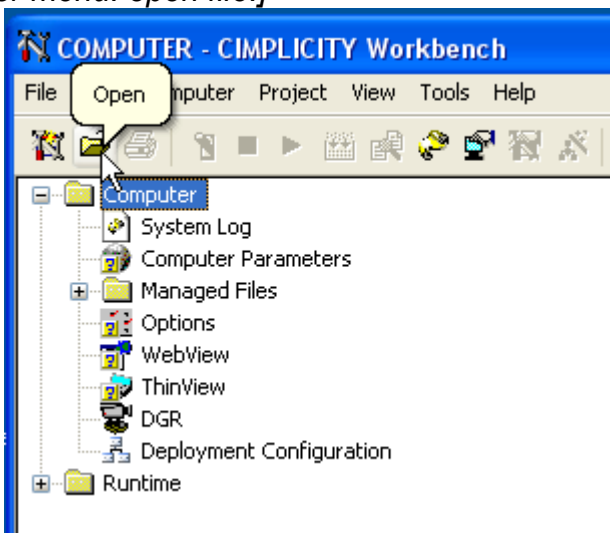
3 Przebieg ćwiczenia *[Exercise]*

1. Zapoznać się z budową stanowiska oraz elementami aktywnymi takimi jak czujniki, lampki, wyświetlacze i przetworniki.
   [You should read how the laboratory station work. Get the information about active elements like lights, displays and converters.]
2. Uruchomić środowisko Proficy Cimplicity HMI/WORKBENCH.
   [Run Proficy Cimplicity HMI/WORKBENCH.]



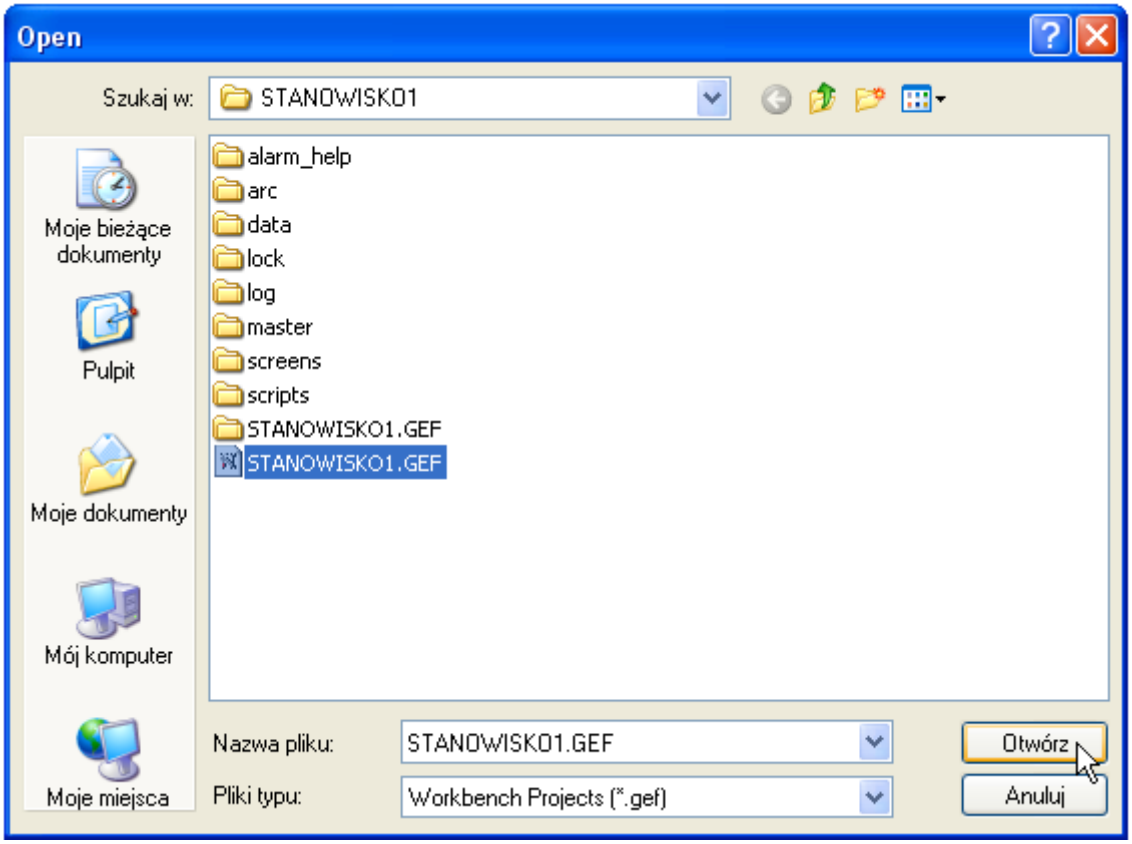
3. Wybrać menu otwierania plików.

   [Choose for menu: open file.]



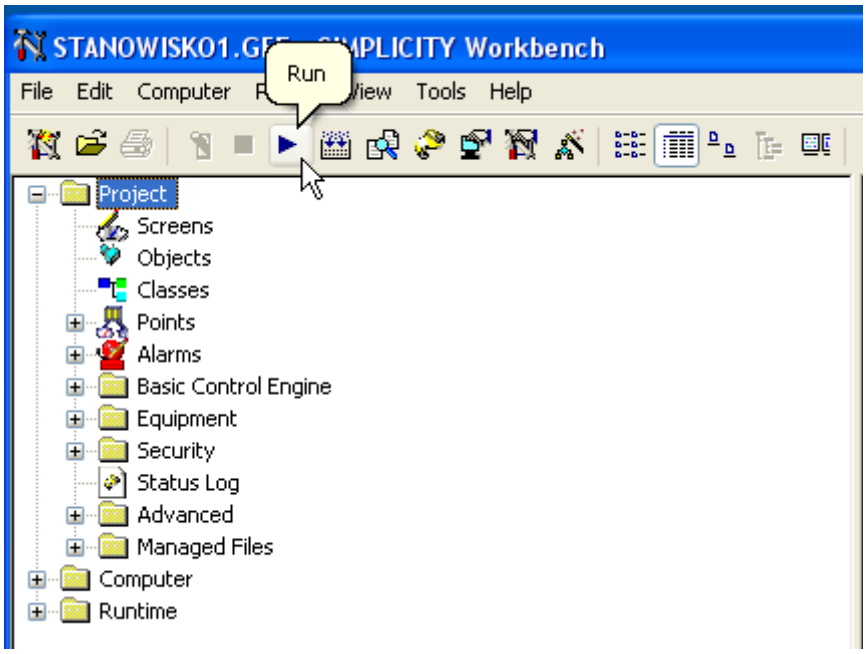
4. Otworzyć plik STANOWISKO2.GEF.

   [Open file: STANOWISKO2.GEF.]



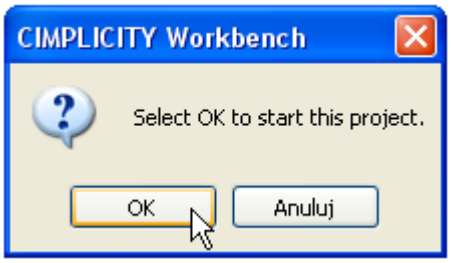
5. Uruchomić symulację przyciskiem Run.

   [Run the simulation.]



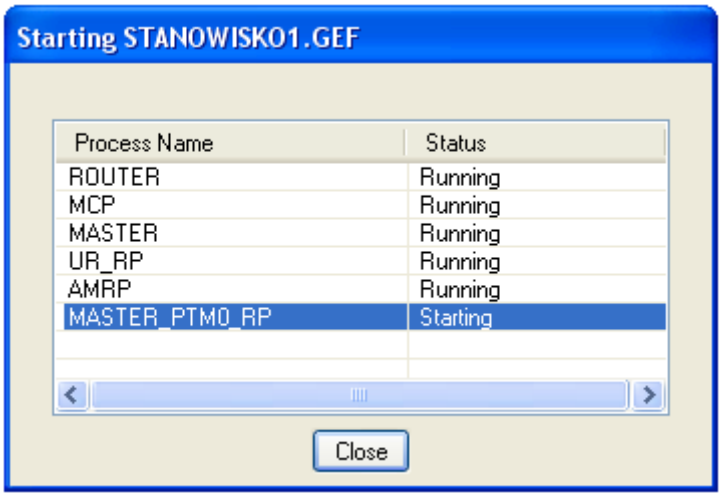
6. Potwierdzić przyciskiem OK.

   [Confirm with OK.]



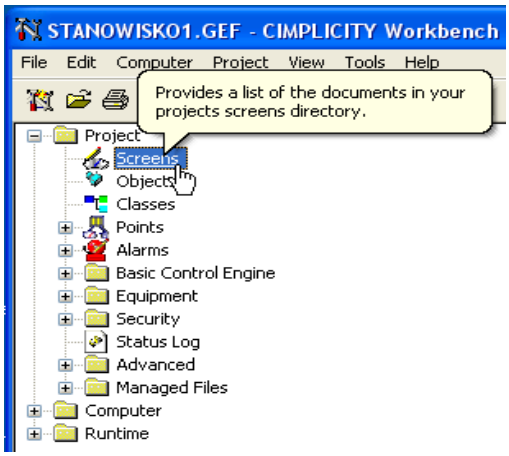
7. Powinno nastąpić uruchamianie poszczególnych modułów.

   [The modules should be run.]



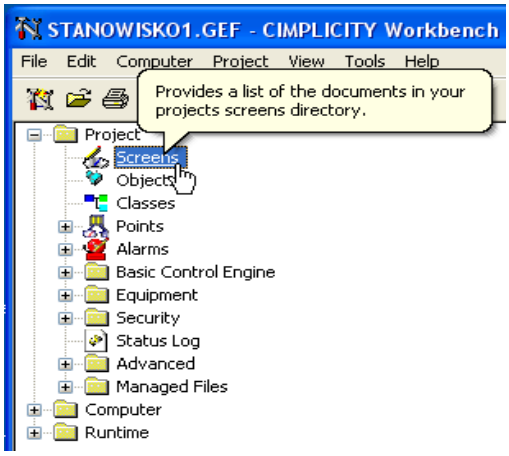
8. Wybrać zakładkę SCREENS.

   [Select the tab: SCREENS.]



9. Dwa razy kliknąć „Stanowisko1.cim”.

   [Double click „Stanowisko1.cim”.]

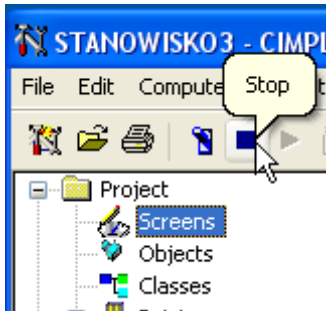


10. Sprawdzić działanie elementów aktywnych. Uzupełnić połączenia na schemacie.

    [Check modules. Complete electric circuit.]

11. Wyłączyć symulację.

    [Stop the simulation.]



12. Potwierdzić wyłączenie przyciskiem OK.

[Confirm with OK.]