biuletyn
automatyki

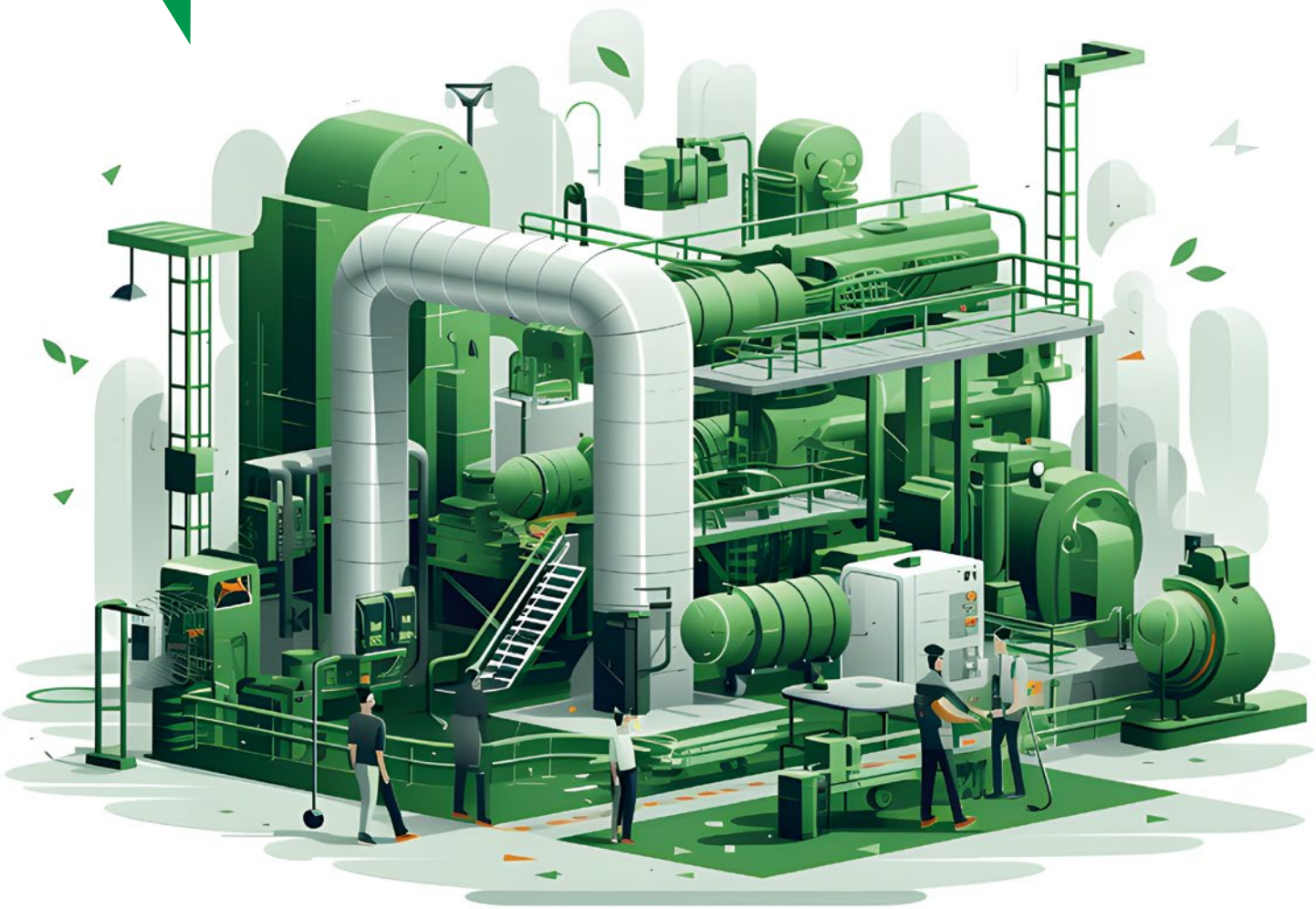
ASTOR

nr 104
jesień 2023
ISSN: 1507–3890

www.astor.com.pl/biuletyn

→ Analiza predykcyjna

Jak skutecznie zapobiegać awariom? – str. 9



„Systemy sterowania związane z infrastrukturą krytyczną, z uwagi na ich kluczowe znaczenie dla bezpieczeństwa i funkcjonowania organów administracji publicznej, są pod specjalnym nadzorem. Wybór dostawcy ma kluczowe znacznie. Globalne marki dają użytkownikom poczucie bezpieczeństwa."

– Piotr Adamczyk, Menedżer produktów Emerson

→ Systemy automatyki w obiektach infrastruktury krytycznej (s. 13)

→ Jak budować cyberbezpieczne aplikacje w oparciu o oprogramowanie AVEVA? (s. 19)

→ Wysokowydajne sterowniki PLC Astraada One Modular oparte na Raspberry Pi® (s. 25)

→ Coboty – współpraca człowieka z robotem, jakiej jeszcze nie było (s. 53)

ASTORINO

ROBOT EDUKACYJNY DO NAUKI PROGRAMOWANIA ROBOTÓW PRZEMYSŁOWYCH

Zobacz więcej

www.astorino.com.pl

astorino Kawasaki Robotics

ZAPROJEKTOWANY I WYPRODUKOWANY W POLSCE

REWOLUCJA W NAUCZANIU ROBOTYKI PRZEMYSŁOWEJ

biuletyn **automatyki**

104 2/2023

AKTUALNOŚCI

Emerson numerem 1 w plebiscycie „Readers' Choice Awards" magazynu Control **5**

Makra EPLAN dla Astraada DRV24 i DRV28A **5**

Robot edukacyjny Astorino – kurs dla początkujących **6**

ASTOR wśród laureatów prestiżowego konkursu Najlepsze Miejsca Pracy Polska 2023 **6**

ASTOR i AGH w Krakowie z umową o współpracy. Biznes dla nauki – nauka dla biznesu **7**

Jak skopiować fabrykę, czyli cyfrowy bliźniak 4.0 w białej księdze od ASTOR **8**

TECHNOLOGIE, PRODUKTY, ZASTOSOWANIA

Analiza predykcyjna: jak skutecznie zapobiegać awariom? **9**

Systemy automatyki w obiektach infrastruktury krytycznej – na co zwrócić uwagę wybierając rozwiązania do takich zastosowań? **13**

Jak budować cyberbezpieczne aplikacje w oparciu o oprogramowanie AVEVA? **19**

Transport hybrydowy w zasięgu ręki. End of line z użyciem robotów mobilnych (AMR) **23**

Wysokowydajne sterowniki PLC Astraada One Modular oparte na Raspberry Pi® **25**

Czy opłaca się inwestować w sterowniki PLC z dwoma rdzeniami? Porównanie sterowników z jednym i dwoma rdzeniami **28**

Jak korzystać z połączenia FTP i VNC w panelach Astraada HMI? **31**

Windows IoT czy Professional? Jaki system operacyjny wybrać dla komputera przemysłowego? **35**

Na co zwrócić uwagę przy doborze falownika do fotowoltaiki? **38**

Konfiguracja sprzętowa kontrolera PACSystems RSTi-EP. Konfiguracja komunikacji w kontrolerze. Kurs programowania PACSystems RSTi-EP CPE200 **40**

Tworzenie projektów w CODESYS ze sterownikami bezpieczeństwa Safety. Kurs programowania w CODESYS **42**

Komunikacja EtherCAT – konfiguracja w środowisku CODESYS. Kurs obsługi i konfiguracji serwonapędów Astraada SRV **46**

Jak przeprowadzić serwis robota przemysłowego? **52**

Coboty – współpraca człowieka z robotem, jakiej jeszcze nie było **53**

REFERENCJE

Sterownik Astraada One w wielkogabarytowej drukarce 3D do zadań konstrukcyjnych **56**

Panele Astraada HMI w mobilnych kurnikach KROPPER **58**

OSTATNIE STRONY

Ludzie ASTORa (104) **63**

Kłaniam się nisko!

Za oknem październik. Większość ludzi, których znam, nie lubi października. „Tylko listopad jest gorszy” – mówią. Nie mogę się z tym zgodzić. Bardzo lubię ten okres roku. Prawda, jest coraz ciemniej i coraz zimniej. Prawda, często pada deszcz. A jednak mam wrażenie, że wszystko teraz toczy się szybciej i łatwiej, niż w upalnych i leniwych letnich miesiącach. I bardziej chce się działać. Działajmy zatem!

Co tym razem znajdą Państwo w „Biuletynie Automatyki”? Bartłomiej Hebda i Mateusz Zajchowski przybliżają ciekawy temat analizy predykcyjnej, która ułatwia skuteczne zapobieganie awariom w przemyśle – a tym samym pozwala niejednokrotnie zaoszczędzić sporo pieniędzy. Polecam również artykuł Piotra Adamczyka o systemach automatyki w obiektach infrastruktury krytycznej, z którego dowiemy się, na co warto zwrócić uwagę wybierając rozwiązania dla takich obiektów. Pokrewny temat porusza Marcin Woźniczka wyjaśniający, jak budować cyberbezpieczne aplikacje w oparciu o oprogramowanie AVEVA.

Z kolei Kinga Tarsa zabiera nas na końcówki linii produkcyjnych i pokazuje, jak transport hybrydowy z wykorzystaniem robotów mobilnych pomaga zoptymalizować proces produkcyjny, zwiększyć jakość, a jednocześnie zmniejszyć koszty. Dużo miejsca poświęcamy modułowym sterownikom PLC Astraada One, o których opowiada Mateusz Pytel.

Publikujemy również wywiad z Radosławem Kołaczem, który wyjaśnia, czym są coboty i co potrafią. W tym numerze znajdą Państwo również sporo praktycznej, inżynierskiej wiedzy. Opisujemy, jak konfigurować protokół EtherCAT w serwonapędach Astraada SRV, jak projektować aplikacje ze sterownikami bezpieczeństwa Astraada One Safety, a także jak przeprowadzić konfigurację sprzętową kontrolera Emerson PACSystems RSTi-EP CPE200.

Bardzo polecam również lekturę artykułu o mobilnych kurnikach polskiej firmy KROPPER. Ta niezwykle ciekawa aplikacja pokazuje, że sterowniki PLC i panele HMI znajdują swoje miejsce nie tylko w zakładach przemysłowych, ale również w rolnictwie. Przyznam szczerze – nie wiedziałem dotąd, że istnieje coś takiego, jak mobilne kurniki. Tym bardziej zautomatyzowane mobilne kurniki. Człowiek uczy się całe życie.

Zapraszam do lektury!
Mateusz Pierzchała
Redaktor naczelny

Zespół redakcyjny:

Piotr Adamczyk
Menedżer produktów Emerson
piotr.adamczyk@astor.com.pl

Michał Januszek
Specjalista ds. systemów sterowania
michal.januszek@astor.com.pl

Marek Niewiadomski
Wynalazca i konstruktor robota Astorino, Główny projektant
marek.niewiadomski@astor.com.pl

Mateusz Fas
Specjalista ds. sprzedaży internetowej
mateusz.fas@astor.com.pl

Renata Poreda
Menedżer ds. komunikacji i PR
renata.poreda@astor.com.pl

Małgorzata Radzik
Młodszy specjalista ds. marketingu AVEVA
malgorzata.radzik@astor.com.pl

Arkadiusz Rodak
Menedżer ds. oprogramowania przemysłowego
arkadiusz.rodak@astor.com.pl

Karolina Tracz
Młodszy specjalista ds. marketingu
karolina.tracz@astor.com.pl

Joanna Kowalkowska
Starszy specjalista ds. marketingu i PR, Menedżer produktu Astorino
joanna.kowalkowska@astor.com.pl

Mateusz Pytel
Menedżer produktu Astraada One
mateusz.pytel@astor.com.pl

biuletyn **automatyki**

Redaktor naczelny:
Mateusz Pierzchała

Korekta:
Mateusz Pierzchała
Michał Zieliński

Redaktor techniczny:
Jacek Gruszczyński

DTP: CleverMinds
info@cleverminds.pl

Prenumerata:
biuletyn@astor.com.pl

Adresy email do pracowników firmy ASTOR mają postać:
imie.nazwisko@astor.com.pl

Wydawca:
ASTOR Sp. z o.o.
ul. Smoleńsk 29; 31–112 Kraków

tel. 12 428 63 70; fax 12 428 63 79
biuletyn@astor.com.pl
www.astor.com.pl

Druk:
Print Management Toruń
Nakład: 1750 egz.
Numer zamknięto: 17.10.2023

Redakcja zastrzega sobie prawo do adiustacji i skracania tekstów, oraz do zmiany tytułów.
Wszelkie prawa autorskie zastrzeżone.

Przedruk tekstów oraz udostępnianie ich w mediach elektronicznych wymaga zgody redakcji.

ASTOR

ASTOR Centrala
ul. Smoleńsk 29; 31–112 Kraków
tel. 12 428 63 00; fax 12 428 63 09
e-mail: info@astor.com.pl

ASTOR Wschód, Gdańsk
ul. Kręta 1, 80–217 Gdańsk
tel. 22 569 56 50; fax 22 569 56 59
e-mail: wschod@astor.com.pl

ASTOR, Oddział Katowice
ul. Żeliwna 38; 40-599 Katowice
tel. 32 355 95 90; fax 32 355 95 99
e-mail: katowice@astor.com.pl

ASTOR, Oddział Kraków
ul. Smoleńsk 29; 31–112 Kraków
tel. 12 428 63 60; fax 12 428 63 69
e-mail: krakow@astor.com.pl

ASTOR Zachód, Poznań
ul. Żniwna 12a; 61–663 Poznań
tel. 61 871 88 00; fax 61 871 88 09
e-mail: poznan@astor.com.pl

ASTOR Wschód, Warszawa
ul. Sielecka 35; 00-738 Warszawa
tel. 22 569 56 50; fax 22 569 56 59
e-mail: wschod@astor.com.pl

ASTOR Zachód, Wrocław
ul. Strachowskiego 12; 52–210 Wrocław
tel. 71 332 94 80; fax 71 332 94 89
e-mail: wroclaw@astor.com.pl

ASTOR Zachód, Szczecin
ul. Cyfrowa 6; 71-441 Szczecin
tel. 91 578 82 80; fax 91 578 82 89
e-mail: szczecin@astor.com.pl

→ Emerson numerem 1 w plebiscycie „Readers' Choice Awards" magazynu Control

Firma Emerson jest prawdziwym liderem technologii automatyzacji w USA. Emerson zdobywa 35 pierwszych miejsc w plebiscycie magazynu Control jako preferowany dostawca w zakresie kontroli procesów i oprzyrządowania – wśród użytkowników i specjalistów w dziedzinie automatyki z całego świata.

W edycji 2022 prestiżowego plebiscytu „Readers' Choice Awards", organizowanego przez magazyn Control firma Emerson została uznana za najlepszego dostawcę aż w 35 kategoriach, zdobywając najwięcej nagród za pierwsze miejsce spośród wszystkich dostawców w branży automatyki. Redaktorzy czasopisma przeprowadzili ankietę wśród setek użytkowników końcowych i firm inżynierskich w całych Stanach Zjednoczonych i na całym świecie, aby stworzyć ranking najlepszych dostawców w zakresie konkretnych kategorii technologicznych. Firma Emerson zdobyła 55 pierwszych, drugich i trzecich miejsc w ponad 80 wymienionych kategoriach, czyli ponad dwukrotnie więcej niż jej najbliższy konkurent.

Emerson okazał się m.in. najlepszym dostawcą w obszarze „Process Automation", zwyciężając w kategoriach „Batch Process Automation" oraz „Continuous Regulatory Control", a w 4 kolejnych zajmując drugie miejsce. W obszarze „Application Software" Emerson zwyciężył w 6 kategoriach z 11: „Advanced Process Control", „Calibration Management", „Loop Tuning", „Alarm Management", „Simulation and Modeling" oraz „Asset Performance Management".

„Rok po roku nasi czytelnicy uznają firmę Emerson za jednego z najbardziej godnych zaufania dostawców technologii automatyzacji procesów – i rok 2022 nie jest tu wyjątkiem" – skomentował Keith Larson, wiceprezydent Putnam Media, wydawcy magazynu Control.

„Użytkownicy końcowi szczególnie cenią dostawców, którzy wprowadzają ważne innowacje w szerokim spektrum specjalizacji i obszarów technologicznych, aby dzięki temu wspierać swoich klientów w rozwiązywaniu najpoważniejszych problemów" – powiedział Mark Bulanda, dyrektor wykonawczy w firmie Emerson.

„Emerson to jeden z najczęściej wybieranych dostawców rozwiązań do automatyzacji procesów produkcyjnych na polskim rynku. Wykorzystywana technologia i platforma sprzętowa pozwalają dostarczać użytkownikom rozwiązania komplementarne i dopasowane do indywidualnych potrzeb." – komentuje Piotr Adamczyk, dyrektor Działu Rozwoju Sprzedaży w firmie ASTOR, manager produktów Emerson. „Rozwój dostawcy w zakresie technologii Przemysłu 4.0 oraz aspektów związanych z bezpieczeństwem, jakich obecnie oczekują nowoczesne zakłady produkcyjne, pozwala użytkownikom koncentrować się na obszarach optymalizacji, usprawniania produkcji i cyfryzacji zakładów. Warto również podkreślić, że spójność całej oferty Emerson umożliwia kompleksową automatyzację całych zakładów, od warstwy polowej po warstwę nadzorczą. Jakość, niezawodność i funkcjonalność oferty Emerson potwierdzają też nagrody i wyróżnienia, jakie Emerson otrzymuje również na naszym lokalnym rynku" – dodaje. •

→ Makra EPLAN dla Astraada DRV24 i DRV28A

Firma ASTOR udostępniła projektantom i integratorom systemów makra EPLAN dla falowników Astraada z serii DRV24 i DRV28A.

Makra EPLAN to biblioteki, które znacząco usprawniają proces projektowania systemów automatyki i planowania zabudowy szaf sterowniczych. Na ich podstawie przygotowywana jest dokumentacja techniczna oraz schematy elektryczne. Oprócz tego makra dają szybki dostęp do plików z parametrami technicznymi, wymiarują urządzenia oraz pozwalają łatwo osadzić je w widoku zabudowy szafy.

Makra EPLAN dla Astraada DRV24 i DRV28A można bezpłatnie pobrać ze stron pomocy technicznej firmy ASTOR.

Dostępne są również w sklepie internetowym ASTOR. Wystarczy wybrać falownik z rodziny DRV24 lub DRV28A, a następnie przejść do sekcji „Dokumentacja i pliki". •

Rodzina falowników Astraada DRV-28. Źródło: ASTOR

→ Robot edukacyjny Astorino – kurs dla początkujących

Na Poradniku Automatyka premierę miał nowy kurs dla początkujących, w ramach którego można zapoznać się z robotem edukacyjnym Astorino i podstawami jego obsługi.

6-osiowy robot edukacyjny Astorino służy do nauki kwalifikacji ELM.07 i ELM.08 w klasach o profilu technik robotyk, na uczelniach, w centrach kształcenia zawodowego i praktycznego. Dzięki Astorino uczniowie i studenci mogą przygotowywać się do egzaminów zawodowych i do pracy w przemyśle.

W ramach kursu poznajemy robota Astorino i uczymy się go obsługiwać. Omawiane są następujące tematy:

- Unboxing robota.
- Szybki start z robotem edukacyjnym Astorino.
- Obsługa systemu wizyjnego OpenMV.
- Obsługa podajnika z magazynkiem kostek.
- Wyznaczanie przestrzeni roboczej robota Astorino.
- Wyznaczanie układu współrzędnych – metoda 4-punktowa.

- Tryby poruszania się robota Astorino.
- Jak poradzić sobie z utratą komunikacji z programem sterującym.
- Zapisywanie punktów i programów sterujących. •

↳ Kurs dostępny jest bezpłatnie na Poradniku Automatyka: www.astor.com.pl/poradnikautomatyka/robot-edukacyjny-astorino-kurs-dla-poczatkujacych/

→ ASTOR wśród laureatów prestiżowego konkursu Najlepsze Miejsca Pracy Polska 2023

25 maja 2023, Instytut Great Place To Work ogłosił listę Najlepszych Miejsc Pracy Polska 2023. ASTOR, w kategorii firm zatrudniających poniżej 500 osób, znalazł się na 14 miejscu. Wyróżnienie to przyznawane jest firmom, które swoją przewagę konkurencyjną budują w oparciu o wzajemne zaufanie i stwarzają świetne miejsce pracy dla wszystkich pracowników. To, co warte podkreślenia – wpływ na wynik ma ocena samych pracowników i wskaźnik zaufania Trust Index.

ASTOR od blisko 20 lat monitoruje puls organizacji rozumiany jako to, czym organizacja żyje na co dzień, co ważne jest dla jej pracowników i jaki wpływ ma firma na nich a oni na firmę. Od 2013 roku systematycznie bierze udział w badaniu Great Place To Work, a co kilka lat uczestniczy również w konkursie. Do tej pory były to edycje w 2013, 2014 i 2016 roku.

Cieszę się niezmiernie, że znaleźliśmy się w gronie najlepszych z najlepszych. Szczególną satysfakcją napawa mnie tytuł Rzecznika Standardów Etyki – mówi Agnieszka Politańska, członek zarządu ASTOR, dyrektor ds. rozwoju pracowników. – *Wzięcie udziału w konkursie pozwala nam zobaczyć w jakim jesteśmy miejscu w odniesieniu do innych pracodawców w Polsce, w naszej kategorii. Jeśli chodzi o perspektywę wewnętrzną, to coroczne badanie pokazuje, że niezależnie od tego, czy bierzemy udział w konkursie, to zaufanie i poczucie dumy z pracy w ASTOR jest na ponadprzeciętnym poziomie. Od czasu do czasu, dla jeszcze większego wzmocnienia poczucia, że tworzymy coś wspaniałego, wyjątkowego, czegoś z czego możemy być dumni, włączamy się do rywalizacji. Udział w samym konkursie jest więc za każdym razem ekscytujący.*

W tym roku Instytut Great Place to Work przebadał w Polsce 180 organizacji – o 30% więcej niż w roku ubiegłym roku. Na liście laureatów, w kategorii firm średnich, do których należy także ASTOR, znalazło się aż 25 firm. Metodologia konkursu jest obiektywna i stanowi światowy standard. O miejscu na liście decyduje łączna ocena dwóch aspektów: audytu kultury organizacyjnej którego wiodącymi obszarami są: skuteczne przywództwo, powszechna innowacyjność oraz przestrzeganie przez firmę swoich wartości i praktyk HR (Culture Audit©), który stanowi 1/3 oceny oraz wyniku ankiety pracowniczej (wskaźnik zaufania w firmie, Trust Index©), z którego pochodzi aż 2/3 finalnej oceny. Tym samym o tym, czy firma znajdzie się wśród Najlepszych Miejsc Pracy, decydują przede wszystkim jej pracownicy.

W badaniu za 2022 ASTOR osiągnął bardzo wysoki wskaźnik zaufania Trust Index na poziomie 87%. przy frekwencji 95%. Aż 92% pracowników firmy uważa, że ASTOR jest wspaniałym miejscem pracy. •

AUTOR: **Renata Poreda**

→ ASTOR i AGH w Krakowie z umową o współpracy. Biznes dla nauki – nauka dla biznesu

Współdziałanie edukacji z biznesem to nowe możliwości. Łączy ono wiedzę z praktycznym doświadczeniem oraz transferuje najnowsze technologie i informacje o nich do akademickiej dydaktyki. Umowa podpisana 28 września 2023 r. przez Akademię Górniczo-Hutniczą w Krakowie oraz firmę ASTOR to przykład budowania synergii między sektorem gospodarczym a środowiskiem naukowym.

Współpraca z firmą ASTOR obejmuje kilka jednostek: Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej, Wydział Inżynierii Mechanicznej i Robotyki, Wydział Zarządzania oraz Centrum Doskonałości Sztucznej Inteligencji AGH. Takie podejście pozwala na kompleksowość edukacji w zakresie technologii i rozwiązań stosowanych w nurcie Przemysłu 4.0.

Prof. Rafał Wiśniowski, Prorektor ds. Współpracy AGH podkreśla: *Nawiązaliśmy strategiczną współpracę z firmą ASTOR, co otwiera przed nami nowe horyzonty rozwoju i możliwości dla naszych studentów, doktorantów oraz pracowników. To partnerskie porozumienie jest dowodem naszego zaangażowania w przekształcanie teorii w praktykę i wdrażanie innowacyjnych rozwiązań do naszej działalności edukacyjnej, szczególnie w obszarach sztucznej inteligencji, Przemysłu 4.0, robotyzacji oraz zarządzania. Stawiamy kolejny krok w dążeniu do integracji nauki z praktyką, wdrażania najnowszych technologii do procesu dydaktycznego oraz doskonalenia programów nauczania oraz zacieśnienia więzi między światem akademickim a biznesem.*

Główne obszary tej współpracy obejmują:

- **Praktyczne doświadczenia dla studentów AGH**: Studenci będą mieli możliwość odwiedzenia showroomów ASTOR Robotics Center oraz ASTOR Innovation Room, gdzie zapoznają się z najnowocześniejszymi stanowiskami zrobotyzowanymi stosowanymi w przemyśle.
- **Cyfrową bibliotekę wiedzy**: Studenci AGH zyskają dostęp do cyfrowych publikacji spółki ASTOR związanych z Przemysłem 4.0.
- **Współpraca z ekspertami**: Pracownicy ASTOR będą spotykać się ze studentami AGH w celu przekazania wiedzy związanej z Przemysłem 4.0 oraz w poszukiwaniu przyszłych ambasadorów i potencjalnych współpracowników.
- **Dostęp do innowacji**: Zarówno pracownicy, jak i studenci AGH, będą mieli możliwość korzystania z najnowszych technologicznych rozwiązań oferowanych przez ASTOR.

Jak podkreśla Michał Wojtulewicz, wiceprezes ds. finansowych w ASTOR, podpisana umowa to ważny sygnał, że polskie szkolnictwo dostrzega potencjał we współpracy z firmami, które mogą wnieść wartość dla rozwoju przyszłych inżynierów.

Jestem niezwykle dumny z faktu, że współpraca z AGH, jedną z najlepszych uczelni technicznych w Polsce, ma dzisiaj swoje kontinuum i systematycznie powiększa się jej zakres. ASTOR to firma, w której idea dzielenia się wiedzą i współpraca z nauką obecna była niemal od początku jej działania. Liczymy na ciekawe wspólne projekty oraz inspirującą wymianę doświadczeń.

W ramach porozumienia planowane jest również organizowanie wspólnych wydarzeń, takich jak wykłady i spotkania edukacyjne, udostępnienie zaawansowanego sprzętu dla pracowni AGH oraz szkolenia dla kadry uczelni w technologiach oferowanych przez ASTOR. Ponadto strony współpracować będą nad wspólnymi projektami badawczo-rozwojowymi, aplikacjami oraz publikacjami naukowymi.

Obie strony podkreślają, że ich partnerstwo będzie korzystne nie tylko dla studentów i pracowników AGH oraz ASTOR, ale również przyczyni się do wzmocnienia więzi między nauką, a sektorem przemysłowym, przyspieszając tempo innowacji w dziedzinie automatyzacji, robotyzacji i sztucznej inteligencji. •

AUTOR: **Renata Poreda**

→ Jak skopiować fabrykę, czyli cyfrowy bliźniak 4.0 w białej księdze od ASTOR

Czwarta Rewolucja Przemysłowa nie tylko dała technologiczne narzędzia, wręcz zintensyfikowała rozwój wielu wcześniej znanych technologii. Tak jest także w przypadku cyfrowego bliźniaka, który stał się „głównym bohaterem" kolejnej publikacji ASTOR w nurcie Przemysłu 4.0 – „Cyfrowy bliźniak 4.0. Jak budować cyfrowe bazy wiedzy w przemyśle".

ASTOR prezentuje kolejną publikację, tzw. whitepaper, związaną z rewolucją przemysłową 4.0. Tym razem na tapet wzięta została jedna z technologii z koła technologii przemysłu 4.0: cyfrowy bliźniak w kontekście procesów ciągłych, dyskretnych i intralogistycznych, w produkcji wsadowej i hybrydowej oraz cyfrowych kopii robotów.

Cyfrowy bliźniak *(digital twin)*, definiowany jest jako wirtualna reprezentacja realnego obiektu. To koncept, który powstał z początkiem XXI wieku. Ogłoszony w 2002 roku i zaprezentowany jako uzupełnienie systemów do zarządzania cyklem życia produktu tzw. PML pomaga w podejmowaniu optymalnych decyzji biznesowych w takich obszarach jak utrzymanie ruchu, rozbudowa linii produkcyjnych, serwis czy sterowanie realnymi obiektami. Jak przewiduje McKinsey & Company, do 2025 roku rynek cyfrowych bliźniaków osiągnie rekordową wartość 7 miliardów euro, co automatycznie przekłada się na wzrost przychodów firm produkcyjnych, nawet o 10%. Aby tak się stało, potrzebna jest wiedza o samej technologii cyfrowego bliźniaka, a bardziej o tym, jak go stosować, by poprawić kluczowe wskaźniki w firmie produkcyjnej.

Obecnie rynek jest niezwykle dynamiczny i często chaotyczny. Wśród wielu zmiennych, które wpływają na jego funkcjonowanie, ciężko jest wyciągać wnioski i podejmować właściwe decyzje bez wsparcia technologii. Stąd rola cyfrowego bliźniaka, szczególnie w przemyśle będzie stale wzrastać – **uzasadnia Piotr Wilk, lider ds. przemysłu 4.0 w ASTOR, współautor raportu,** i dodaje – *dzięki postępowi technologicznemu mamy coraz szersze możliwości, co przekłada się na coraz większe korzyści wynikające z jego wykorzystania. Jeśli zastosowanie tej innowacji ma uzasadnienie biznesowe, na pewno warto ją poważnie rozważyć.*

Mamy tutaj dwie możliwości. Zastosowanie koncepcji cyfrowych bliźniaków na etapie testowania nowych rozwiązań przed wprowadzeniem ich w życie bez ponoszenia dodatkowych kosztów. Polega to na stworzeniu cyfrowych kopii poszczególnych maszyn, systemów, całych linii produkcyjnych. Druga z możliwości to optymalizacja systemów i procesów już działających na ich cyfrowych kopiach.

Dobierając partnerów do publikacji, ASTOR miał na uwadze kilka aspektów, od wiedzy na temat technologii, przez kompetencje potrzebne do tworzenia cyfrowych modeli i umiejętność ich wdrożenia, aż po znajomość światowych trendów i predykcji.

Z doborem autorów do tej publikacji nie mieliśmy najmniejszego problemu – **mówi Małgorzata Życzkowska, asystentka ds. Przemysłu 4.0 w ASTOR, kierowniczka projektu publikacji** – *współpracujemy bowiem z firmami, które od jakiegoś czasu zajmują się tym innowacyjnym zagadnieniem. Zaprosiliśmy firmę Control-Service, Złotego Partnera ASTOR, która na swoim koncie ma już kilka skutecznych wdrożeń technologii cyfrowego bliźniaka, szczególnie w branżach, gdzie działa produkcja wsadowa. Z kolei FlexSim Intermarium to firma, która cyfrowymi modelami symulacyjnymi usprawnia procesy intralogistyczne w fabrykach. Mamy również rozdział poświęcony cyfrowym bliźniakom procesów zrobotyzowanych, o których pisze Kamil Majcher, zastępca kierownika działu technicznego ASTOR. Podsumowaniem tych praktycznych przykładów są kierunki i najnowsze trendy rozwoju technologii cyfrowego bliźniaka na świecie okiem – Sławomira Tadeji – asystenta badawczego z University od Cambridge. Rozwój cyfrowego bliźniaka nie kończy się przecież w tej publikacji – z dnia na dzień rozwija się on i może usprawniać coraz więcej procesów* – **podsumowuje Małgorzata Życzkowska.**

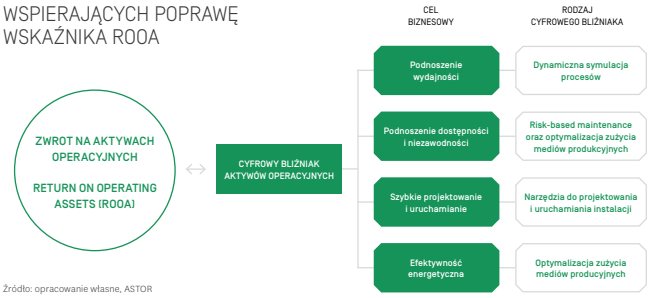
Raport to odpowiedź na najczęściej zadawane pytania w zakresie coraz bardziej złożonych procesów produkcyjnych i logistycznych. To także spojrzenie jak osiągać korzyści biznesowe, takie jak redukcja kosztów, zwiększenie przychodów w procesach ciągłych, dyskretnych, zrobotyzowanych, szczególnie w produkcji dyskretnej i wsadowej. A także w całym łańcuchu dostaw. W przemyśle przyszłości chodzi o coś więcej.

Rosnąca złożoność procesów produkcyjnych wymaga tworzenia ich cyfrowych kopii na coraz wyższych poziomach dojrzałości. „Cyfrowy bliźniak 4.0 Jak budować cyfrowe bazy wiedzy w przemyśle" podpowiada, jak to robić. •

AUTOR: **Renata Poreda**

↳ Czytaj więcej na stronie: www.astor.com.pl/whitepaper-cyfrowy-blizniak-4-0

RODZAJE CYFROWYCH BLIŹNIAKÓW WSPIERAJĄCYCH POPRAWĘ WSKAŹNIKA ROOA



Źródło: opracowanie własne, ASTOR

Korzyści z wdrożenia cyfrowych bliźniaków w produkcji dyskretnej:

Analiza predykcyjna: jak skutecznie zapobiegać awariom?

Nieplanowane przestoje to jeden z najbardziej dolegliwych problemów, jakie zdarzają się w przemyśle. Z pewnością marzeniem każdego działu utrzymania ruchu jest sytuacja, w której wystarczające jest wykonywanie tylko zaplanowanych przeglądów lub serwisów. Niestety tak nie jest – awarie się zdarzają, a to często wiąże się z dużymi kosztami. Drogie może być urządzenie, które uległo awarii, albo też sam przestój generuje poważne straty. Analiza predykcyjna jest odpowiedzią na ten problem.

» Na początek przyjrzyjmy się kilku interesującym statystykom związanym z nieplanowanymi przestojami.

Wyzwania związane z nieplanowanymi przestojami

Przede wszystkim z różnych szacunków wynika, że nawet ponad **80% awarii ma charakter losowy**. Pozostałe niespełna 20% przypadków awarii jest związane z wiekiem urządzeń. Wiedzę dotyczącą starzenia się urządzeń mogą posiadać np. najbardziej doświadczeni operatorzy i inżynierowie, ale z badań firmy Vanson Bourne wynika, że nawet w dużych i nowoczesnych firmach większość operatorów może nie być świadomych, kiedy wymienić, ulepszyć lub konserwować zasoby.

Jak widać, pracownikom często brakuje wiedzy pozwalającej przewidywać awarie. Kiedy coś się zepsuje, wszyscy koncentrują się na jak najszybszym naprawieniu problemu, a rzadko myślą np. o sporządzeniu właściwej dokumentacji. Inna sprawa, że nawet istnienie takiej dokumentacji nie musi pomagać w zapobieganiu awarii, jeżeli zapowiadające ją symptomy są trudne lub niemożliwe do zauważenia.

Równie znamienna jest trzecia statystyka ogólnoświatowego przemysłu. **Średni koszt jednej godziny nieplanowanego przestoju infrastruktury IT to 260 000 dolarów**. Kwota ta robi wrażenie, ale należy pamiętać, że to jest średnia – i dotyczy tylko infrastruktury IT. Zdarza się więc w światowym przemyśle wiele przestojów mniej kosztownych, ale również całkiem sporo takich dużo droższych, gdzie straty mogą sięgać nawet milionów dolarów. To istotne spostrzeżenie, które będzie miało ważny wpływ na planowanie systemu analizy predykcyjnej. Wdrażanie takich systemów warto bowiem zaczynać od tych obszarów, gdzie potencjalne zagrożenie stratami jest najwyższe.

Kończąc przytaczanie statystyk warto wspomnieć też o mniej wymiernych konsekwencjach nieplanowanych przestoju. Poważna awaria może nie tylko skutkować stratami materialnymi, ale być też zagrożeniem bezpieczeństwa dla ludzi lub środowiska. W efekcie może dojść do zdarzeń tragicznych, które dodatkowo będą miały rujnujący wpływ na reputację przedsiębiorstwa i otoczenie.

Predictive maintenance – jak to działa?

Zobaczyliśmy dość jasno, że awarie są nieprzyjemne. Gdyby udało się skutecznie je przewidywać, według różnych szacunków możliwe byłoby ograniczenie kosztów operacyjnych przedsiębiorstw produkcyjnych o 10 do 20%.

W jaki sposób można przewidzieć awarię? Przecież właśnie dowiedzieliśmy się, że jest to zdarzenie, które przytrafia się w sposób losowy. Pozornie właśnie tak jest, ale gdy przyjrzymy się uważniej, dojdziemy do wniosku, że nie do końca. Każda bowiem awaria jest czymś spowodowana, a w praktyce okazuje się, że już wcześniej można dostrzec symptomy, które ją zapowiadają.

Aby dostrzec te symptomy, **potrzebujemy właściwych danych**, zbieranych z procesu produkcyjnego. Dane takie muszą pochodzić z czujników. Wciąż jeszcze zdarza się, że procesy są słabo opomiarowane, ale najczęściej jednak każda linia produkcyjna wyposażona jest w wiele czujników i sygnałów, które w sposób bezpośredni i pośredni

AUTOR: **Bartłomiej Hebda**

Dział IT ASTOR

bartlomiej.hebda@astor.com.pl

AUTOR: **Mateusz Zajchowski**

Specjalista ds. oprogramowania przemysłowego AVEVA

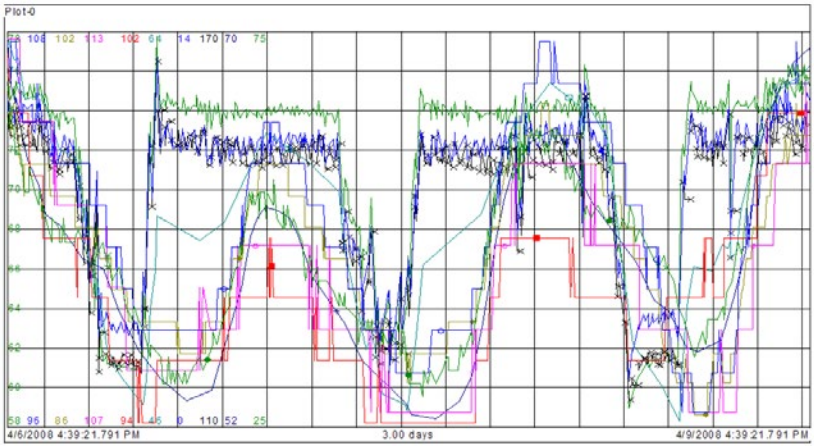
mateusz.zajchowski@astor.com.pl

REDAKTOR TEKSTU: **Mateusz Pierzchała**

Wyzwania związane z nieplanowanymi przestojami. Źródło: AVEVA. Źródła danych: 1) Vanson Bourne 2) Arcweb.com, 3) Aberdeen

wskazują na to, jak pracuje. Dane zbierane z tych czujników mogą być wyświetlane na stacjach operatorskich, a także trafiać do baz danych, np. AVEVA Historian. W bazie danych zbieramy więc całą historię pomiarów, ze stemplami czasowymi. Tych danych z reguły jest bardzo dużo – zależy to od wielkości systemu, liczby czujników i częstotliwości zbierania. Następnie korzystając z odpowiednich narzędzi możemy np. taką historię pomiarów przedstawić na wykresie, takim jak obok.

Jak widać... niewiele tu widać niestety. Analiza takiego wykresu jest bardzo trudna. Nie sposób zauważyć tu drobnych zmian. Nie da się też „nieuzbrojonym okiem" wykryć jakichkolwiek korelacji między sygnałami – nie widzimy bowiem, czy zmiana jednego z sygnałów wpływa na zmianę drugiego. A pokazany powyżej wykres to przecież i tak stosunkowo mało skomplikowany przykład. Jeżeli mielibyśmy przed sobą wykres jednego lub dwóch pomiarów, to być może – mając odpowiednią wiedzę i doświadczenie – bylibyśmy w stanie coś na nim dostrzec. W większości procesów będziemy mieli zapewne do czynienia z dziesiątkami lub setkami pomiarów.



Wykres pomiarów zebranych w bazie AVEVA Historian. Źródło: AVEVA

Monitorowanie sygnałów: podejście tradycyjne

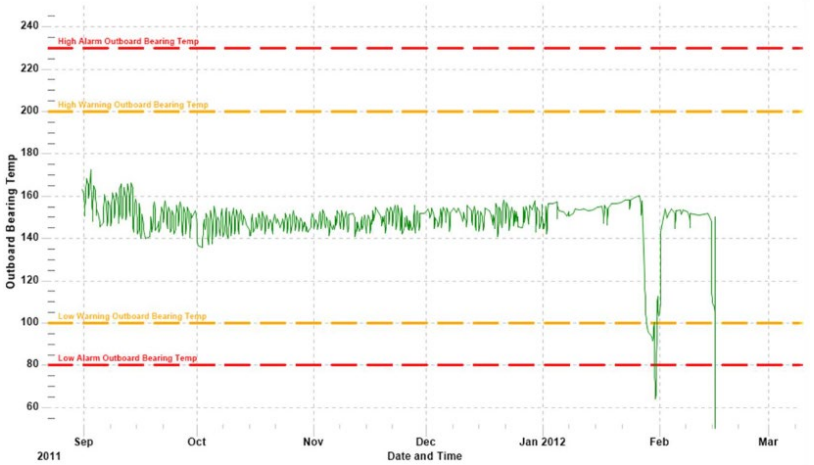
W tradycyjnym podejściu odpowiedzią na ten problem jest **system alarmowy**. Pozwala on dla każdego pomiaru określić zakres, w którym wartość parametru traktowana jest jako poprawna. W przypadku wyjścia poza ten zakres – zgłaszany jest alarm. Przykładowo, dla czujnika temperatury możemy określić, że prawidłowa wartość temperatury wynosi między 100 a 200 stopni. Gdy wartość pomiaru wyniesie ponad 200 (albo poniżej 100), to generowane będzie najpierw ostrzeżenie, a w przypadku większego przekroczenia – alarm. Z całą pewnością tego rodzaju informacja jest przydatna i może ułatwić reakcję na jakiś problem. Jest to jednak rozwiązanie dalekie od ideału.

Po pierwsze – widzimy tylko, że temperatura jest nieprawidłowa. **Nie wiemy, dlaczego**. Jeżeli jednocześnie pojawiają się alarmy z innych czujników lub urządzeń, jest dla nas jasne, że rzeczy idą nie najlepiej. Ale nie wiemy, co konkretnie się zepsuło. Co było pierwotną przyczyną, a co skutkiem.

Drugi problem z alarmami jest natomiast taki, że bardzo często... **jest już za późno**. Jeżeli temperatura TERAZ przekroczyła limit, to prawdopodobnie do awarii doszło już jakiś czas wcześniej – i możemy tylko ratować co się da, np. zatrzymując proces. **Innymi słowy, alarm nie pozwala nam *uniknąć* awarii. Możemy się tylko o niej *dowiedzieć*.**

Dodatkowym problemem przy konfigurowaniu systemu alarmowego może być też samo ustalanie progów dla alarmów, które często są ustalane, kolokwialnie mówiąc, „na oko" – na bazie doświadczenia inżynierów. Nie mogą być ustawione zbyt nisko, bo system byłby zbyt czuły i pojawiałoby się dużo fałszywych alarmów. Ale nie mogą być też ustawione zbyt szeroko, aby nie spowodować realnego zagrożenia.

Dobrym przykładem opisanych wyżej problemów jest wykres przedstawiony poniżej:



Przykładowy wykres temperatury z uwzględnieniem alarmów. Źródło: AVEVA

Wykres pokazuje przebieg temperatury z rozdzielczością miesięczną. Widać wyraźnie, że przebieg temperatury wygląda przez wiele miesięcy podobnie. Natomiast na początku stycznia charakter wykresu wyraźnie się zmienia, sygnał zachowuje się zupełnie inaczej. Już tu można się domyślać, że coś jest nie tak – i to przez cały miesiąc. Alarmu jednak nie ma, bo limity nie są przekroczone.

O tym, że z całą pewnością *coś* jest nie tak, dowiadujemy się dopiero po około miesiącu, gdzie

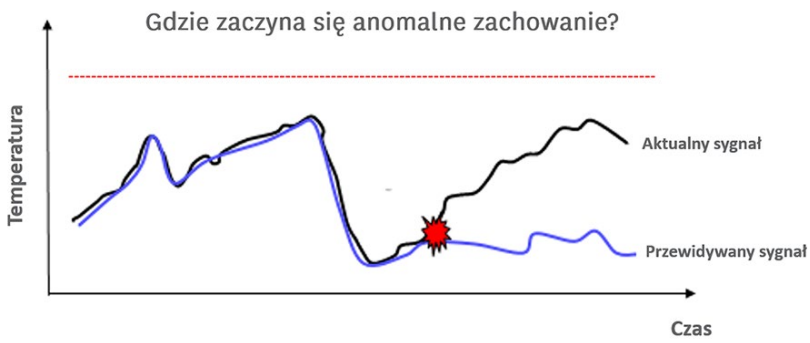
wartość temperatury spada poniżej limitu przyjętego dla alarmów. Wtedy pojawia się alarm, wtedy też – patrząc na wykres – orientujemy się, że przyczyna problemu prawdopodobnie pojawiła się kilka tygodni wcześniej. Nadal jednak nie wiemy, jaka to była konkretnie przyczyna.

Monitorowanie sygnałów: podejście predykcyjne

Podejście predykcyjne różni się radykalnie od tego tradycyjnego, opartego na alarmach. W pewnym uproszczeniu można powiedzieć, że dla każdej maszyny i każdego procesu da się zazwyczaj określić pewien model działania, który moglibyśmy nazwać wzorcowym. To po prostu zapis prawidłowego przebiegu procesu, złożony z szeregu wartości zbieranych pomiarów. Taki model tworzony jest na podstawie zebranych danych historycznych.

Inaczej mówiąc: **algorytmy predykcyjne** uczą się – na podstawie danych historycznych – przewidywać, jaki *powinien być* przebieg sygnału. Tym samym zawsze jest wiadome, jaka powinna być wartość tego sygnału w danej chwili – a jaka powinna być w ciągu najbliższych minut, godzin lub dni.

Ten sygnał predykcyjny jest nieustannie porównywany do rzeczywistego przebiegu sygnału. Gdy tylko te dwa przebiegi zaczynają wyglądać inaczej (a więc rzeczywisty sygnał zaczyna odbiegać od modelowego), natychmiast wiemy, że zaczyna się dziać coś złego.



Wykrywanie anomalii na podstawie porównywania sygnałów. Źródło: AVEVA

Wracając do naszego przykładowego pomiaru temperatury, algorytm predykcyjny „dostrzegłby" problem już na początku stycznia – bo to właśnie tam przebieg sygnału zaczyna wyglądać zupełnie inaczej. Dzięki temu możemy zareagować natychmiast – tak naprawdę niemal miesiąc przed faktycznym wystąpieniem awarii!

Analiza predykcyjna daje czas na spokojną reakcję

Dzięki analizie predykcyjnej niemal natychmiast wiemy o każdym pojawiającym się problemie. **Mamy więc czas**, aby zaplanować i przeprowadzić niezbędne działania naprawcze. Możemy np. niezwłocznie wymienić jakieś urządzenie lub część, możemy też podjąć świadomą decyzję o niepodejmowaniu żadnych działań (gdyż np. wiemy, że w krótkim czasie zaplanowany jest przegląd albo serwis maszyny).

Warto tu jeszcze wspomnieć o czułości algorytmu predykcyjnego. Jeżeli badamy odchylenie sygnału rzeczywistego od wzorcowego, możemy zadecydować, jaka będzie dokładność tego badania. Innymi słowy – jak duże odchylenie spowoduje wygenerowanie alarmu. W takim przypadku niewielkie odchylenia nie spowodują alarmu, ale gdy przekroczą określoną skalę – alarm się pojawi.

Mapa kondycji urządzenia

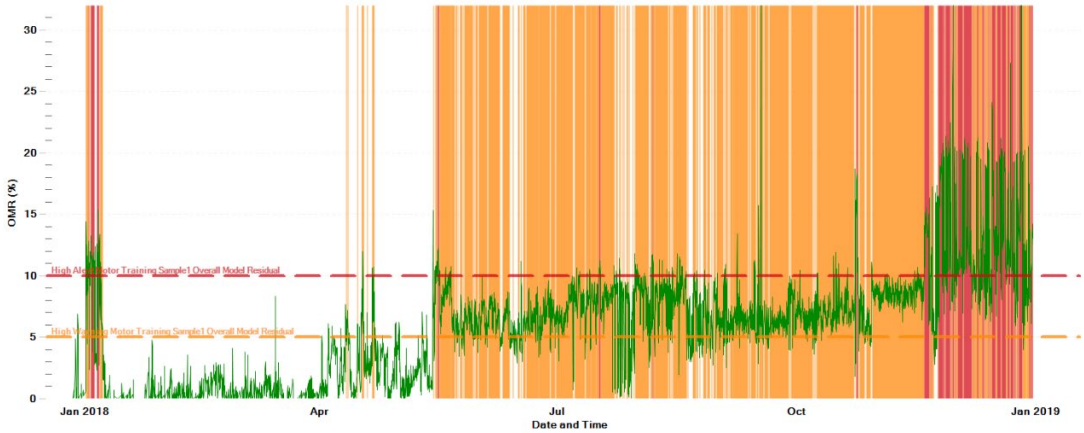
Dzięki algorytmom predykcyjnym możemy zbudować tzw. **mapę kondycji urządzenia**. Jest to specjalny rodzaj wykresu ilustrujący przebieg monitorowanego sygnału, pokazującego dodatkowo, w których okresach sygnał był nadmiernie odchylony od normy – i jak bardzo. Obszary umiarkowanego odchylenia oznaczane są kolorem żółtym, a tam, gdzie odchylenie było znaczące, pojawia się kolor czerwony.

Nie można zapominać, że na całościową kondycję wpływ może mieć np. kilkadziesiąt sygnałów, które opisują pracę danego urządzenia. Nie musimy jednak martwić się tym, jak znaleźć korelacje między tymi sygnałami. Odpowiednie algorytmy zajmą się tym w sposób automatyczny, dzięki czemu otrzymujemy wiodący sygnał, który przyczynił się najbardziej oraz sygnały, które w mniejszym stopniu przyczyniły się do powstania anomalii.

Natomiast w momencie wystąpienia alarmu mamy dostęp do kompletu danych. Algorytm wskazuje nam, które konkretnie sygnały mają największy wpływ na to, że kondycja urządzenia w danej chwili nie jest dobra. Możemy zobaczyć, które parametry i w jakim stopniu wpływały na pojawienie się problemu. Jest to więc narzędzia do tego, aby łatwo odnaleźć główną przyczynę problemów z urządzeniem.

AVEVA Predictive Analytics – analiza predykcyjna w praktyce

Fundamentem wykonywania analiz predykcyjnych jest gromadzenie historycznych pomiarów. Mając dane możemy wykorzystać algorytmy, które pozwalają je analizować i na bieżąco wykrywać pojawiające ▷



Przykładowa mapa kondycji urządzenia. Źródło: AVEVA

Kolejne kroki po wykryciu anomalii. Źródło: AVEVA

się anomalie. Aby jednak powstał kompleksowy system pozwalający na zapobieganie awariom, potrzebne jest jeszcze coś. Potrzebujemy narzędzia, które pozwoli przełożyć wiedzę o zagrożeniu awarią na konkretne działania. Potrzebujemy aplikacji, która pomoże rozdystrybuować zadania pomiędzy osobami odpowiedzialnymi za poszczególne obszary, a także ułatwi gromadzenie wiedzy o problemach technicznych i sposobach ich rozwiązywania.

Takim narzędziem jest **AVEVA Predictive Analytics**, który implementuje cały proces analizy predykcyjnej:

- wykrycie zdarzenia na podstawie analizy odchylenia sygnału rzeczywistego od wzorcowego,
- analiza przyczyn anomalii i wpływu poszczególnych sygnałów na kondycję urządzenia,
- tworzenie zgłoszeń serwisowych,
- rozdysponowanie zadań serwisowych dla pracowników,
- monitorowanie przebiegu akcji serwisowej,
- gromadzenie dokumentacji dokonanych napraw.

AVEVA Predictive Analytics umożliwia nam śledzenie każdego przypadku krok po kroku, z jednoczesnym budowaniem bazy wiedzy technicznej, zawierającej komplet informacji o awariach, ich przyczynach oraz sposobach ich usunięcia. Taka baza jest bardzo przydatna, jeżeli możliwe jest powtórzenie się podobnych zdarzeń w przyszłości, a także w przypadku, gdy mamy wiele takich samych urządzeń, na których mogą zdarzać się analogiczne awarie. •

AVEVA Predictive Analytics. Źródło: AVEVA

Systemy automatyki w obiektach infrastruktury krytycznej – na co zwrócić uwagę wybierając rozwiązania do takich zastosowań?

Na inżynierach pracujących przy systemach sterowania związanych z infrastrukturą krytyczną spoczywają szczególne obowiązki. Pozornie to takie same systemy, jak w każdej innej branży, ale z uwagi na ich kluczowe znaczenie dla bezpieczeństwa i funkcjonowania organów administracji publicznej są one pod specjalnym nadzorem. Budowa, uruchomienie, serwis i utrzymanie takich obiektów wymagają od służb odpowiedzialnych za nie pełnej dostępności oraz doświadczenia pozwalającego na utrzymanie obiektów w należytym stanie.

» Niestety, coraz większa złożoność takich obiektów oraz architektura pracy, która coraz częściej ma charakter rozproszony, stawia przed systemami infrastruktury krytycznej kolejne wyzwania. Z uwagi na charakter swojego działania oraz znaczenie dla prawidłowego funkcjonowania państwa **systemy takie pracują w trybie ciągłym**, a to oznacza, że sposób ich obsługi wymaga innych procedur i procesów, aby nie dopuścić do ich zatrzymania.

Systemy infrastruktury krytycznej, które uważa się w Polsce za kluczowe dla bezpieczeństwa państwa i jego obywateli, to systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności i sieci teleinformatycznych,
- finansowe,
- ochrony infrastruktury krytycznej,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągi substancji niebezpiecznych).

Jak widać, obiekty te funkcjonują w różnych sektorach i **muszą być przygotowane do elastycznego skalowania** w zależności

AUTOR: **Piotr Adamczyk**
Dyrektor Działu Rozwoju Sprzedaży
Menedżer produktów Emerson
piotr.adamczyk@astor.com.pl

od tego, ilu obywateli z nich korzysta. Branża „wod-kan" musi gwarantować dostęp do wody pitnej dla każdego mieszkańca, co przy dynamicznym rozwoju dużych miast wymaga elastycznego zwiększania produkcji wody w zależności od zapotrzebowania. Branża ciepłownicza z kolei musi reagować na bieżąco na zapotrzebowanie na ciepło, które zależy od pory roku, temperatury na zewnątrz, dostępnych paliw.

Dla takich obiektów Rządowe Centrum Bezpieczeństwa wydaje materiały informujące, w oparciu o jakie standardy i dobre praktyki takie systemy budować, aby w kontekście ich znaczenia zagwarantować najwyższy poziom dostępności i niezawodności.

A jak to wspierają producenci automatyki?

No właśnie. Czy tylko na inżynierach obsługujących takie systemy ciąży odpowiedzialność za ich bezawaryjną pracę? W dużej części tak, ale wybór dobrze przemyślanych rozwiązań w zakresie automatyzacji może pośrednio w znaczący sposób wesprzeć inżynierów, którzy za te systemy odpowiadają. Na co zatem warto zwrócić uwagę wybierając i użytkując takie systemy? Jest kilka elementów, które warto wziąć pod uwagę.

Zaufany producent – poczucie bezpieczeństwa

Wybór dostawcy może tu mieć kluczowe znacznie. **Globalne marki mogą dawać użytkownikom poczucie bezpieczeństwa**. Funkcjonują w oparciu o ogólnie przyjęte standardy, które porządkują wiele procesów. Na przykład cykl życia produktów: tworzenie systemów, ich utrzymywanie, rozwój, serwis i na końcu wycofanie z oferty jest ściśle określonym procesem. Tu nie ma miejsca na przypadki. Każdy krok jest dokładnie przemyślany, aby zagwarantować użytkownikom maksimum bezpieczeństwa.

To dbanie o bezpieczeństwo użytkownika przejawia się chociażby w **wydawaniu aktualizacji oprogramowanie układowego na bieżąco**, oraz nieustanne monitorowanie podatności na czynniki zewnętrzne, w tym cyberataki. Dedykowane podmioty odpowiedzialne za testowanie rozwiązań przemysłowych (CERN) wydają szereg rekomendacji, które nakładają na producentów konieczność aktualizacji oprogramowania, aby podatności usunąć.

*Bardzo istotne znaczenie z punktu widzenia systemów automatyki dla infrastruktury krytycznej ma **kompleksowa oferta**. Możliwość zbudowania całego systemu w oparciu o komponenty pochodzące od jednego dostawcy daje użytkownikom pewność, że urządzenia będą ze sobą współpracować, mają przygotowane mechanizmy wymiany danych między sobą oraz – co bardzo ważne – są programowane i konfigurowane z jednego oprogramowania narzędziowego.*

Często jest to związane z koniecznością dostępu do najnowszych technologii, które w tych konkretnych przepadkach mają olbrzymie znaczenie dla użytkowników tych systemów. O tym, jak bardzo są one niezawodne, może świadczyć chociażby **gwarancja, która w przypadku firmy Emerson wynosi w standardzie 5 lat dla produktów z rodziny PACSystsms RX3i**. Bezpieczeństwo potwierdzają również certyfikaty, chociażby Achilles Level 2.

Kompleksowa oferta

Bardzo istotne znaczenie z punktu widzenia systemów automatyki dla infrastruktury krytycznej ma **kompleksowa oferta**. Możliwość zbudowania całego systemu w oparciu o komponenty pochodzące od jednego dostawcy daje użytkownikom pewność, że urządzenia będą ze sobą współpracować, mają przygotowane mechanizmy wymiany danych między sobą oraz – co bardzo ważne – programowane i konfigurowane są z jednego oprogramowania narzędziowego (co znacząco przyspiesza proces wdrożenia). Budowa różnych architektur w oparciu o te same komponenty daje też inżynierom pełną elastyczność przy budowaniu systemu, dopasowując go technicznie do potrzeb każdego obiektu w każdej branży.

W tym aspekcie oferta Emerson jest naprawdę mocno rozbudowana. Będąc drugim największym dostawcą (w ujęciu globalnym) firma ta inwestuje w nowe technologie i rozbudowuje swoją ofertę tak, aby być w stanie kompleksowo dostarczyć cały system sterowania. Od urządzeń polowych, przez układy wejść-wyjść, sterowniki PLC, kontrolery, systemy bezpieczeństwa, urządzenia do lokalnej wizualizacji procesów, ale też urządzenia komunikacyjne, napędowe oraz – co wymusza czwarta rewolucja przemysłowa – dedykowane **urządzenia do przetwarzania brzegowego**.

Łatwe programowanie i wdrożenie

Szeroka, kompleksowa oferta – aby spełniała swoją rolę z wykorzystaniem wszystkich funkcji – wymaga narzędzia, które pozwoli cały system skonfigurować i uruchomić. System ten komplikuje się znacząco wraz ze wzrostem liczby urządzeń, które wchodzą w jego skład. Na inżynierach spoczywa odpowiedzialność za ich właściwe połączenie. Zarządzanie wieloma różnymi narzędziami i ich wersjami jest bardzo skomplikowane i wymagające. Dlatego w dużych systemach warto korzystać z **kompleksowych rozwiązań, które konfigurowane są z poziomu jednego narzędzia**. To znacząco usprawnia proces konfiguracji i programowania.

Jedno narzędzie pozwala także zachować kompatybilność urządzeń względem siebie. Jeden silnik dla wszystkich rodzin kontrolerów pozwala wykorzystać ten sam kod programu i te same funkcje na różnych platformach sprzętowych. System rośnie wraz ze wzrostem oczekiwań względem niego – możemy przenosić kod programu na inne rodziny kontrolerów, wykorzystując posiadany program z gwarancją jego kompatybilności. Wbudowane w oprogramowanie funkcje są obsługiwane dokładnie tak samo w każdej serii kontrolera, a możliwość tworzenia swoich własnych struktur pozwala na ich przenoszenia bez konieczności modyfikacji.

Dlaczego to jest tak ważne w systemach infrastruktury krytycznej? Z uwagi na

walidację projektów. Skoro mamy przygotowany działający i zwalidowany algorytm, który działa, przenosząc go na inną platformę sprzętową nie musimy tego wykonywać po raz kolejny, co znacząco przyspiesza cały proces oraz minimalizuje ryzyko powstania błędów. W praktyce system przygotowany np. na PACSystems RSTi-EP można bez problemu przenieść na kontroler RX3i. Jeśli pojawia się taka potrzeba i system wymaga pracy w architekturze redundantnej, również wykorzystamy ten sam kod programu.

Łatwa rozbudowa systemu

Większość systemów po jakimś czasie wymaga rozbudowy. Szczególnie dotyczy to systemów w infrastrukturze krytycznej. Rozbudowa takich systemów jest bardzo wymagającym procesem. Nie mówimy tutaj o dołożeniu kolejnego pomiaru do systemu, a o rozbudowie o kolejne podsystemy, zwiększające funkcjonalność całego obiektu.

Wraz ze wzrostem rozmiarów systemu konieczna jest często zmiana rodziny kontrolerów na większe, z większymi zasobami i wydajnościami. Czasem trzeba przeprojektować architekturę całości. W takim przypadku bardzo istotna jest **możliwość wykorzystania posiadanych urządzeń, wiedzy i aplikacji**.

Z uwagi na ciągły charakter pracy takich obiektów rozbudowa często realizowana jest „na ruchu". Nie zawsze każdy proces technologiczny można rozbudować na ruchu – to jest oczywiste. Ale nie zawsze rozbudowa wiąże się ze zmianą technologii produkcji i potrzebą zatrzymania instalacji. Wszędzie tam, gdzie nie ma czasu na czekanie na planowany przestój pracy obiektu, powinniśmy inwestować w układy automatyki, które na taką rozbudowę na ruchy będą pozwalały.

W przypadku Emerson **wszystkie urządzenia PACSystems mają możliwość programowania na ruchu** z wykorzystaniem funkcji *Test Mode*. Obiekty infrastruktury krytycznej wyposażone w redundantne kontrolery mają także możliwość zmiany konfiguracji sprzętowej na ruchu, co oznacza możliwość dokładania kolejnych elementów do systemu i wpinanie ich do pracy bez zatrzymywania całego ciągu technologicznego.

Architektura chroniąca przed nieplanowanym przestojem

Redundantna architektura to kolejna domena systemów automatyki procesowej w infrastrukturze krytycznej. Firma Emerson jest w tym zakresie liderem w branży, wykorzystując swoje ponad 30-letnie doświadczenia w projektowaniu systemów wysokiej dostępności. Takie systemy chronią nas przed nieplanowanym przestojem, wynikającym z awarii dowolnego komponentu. W takim przypadku sterowanie przekazywane jest do urządzeń rezerwowych, które w sposób niezauważalny z punktu widzenia ciągłości procesu produkcyjnego przejmują nad nim kontrolę, dając czas inżynierom na lokalizację przyczyn i eliminację awarii.

Czym oferta Emerson wyróżnia się od alternatywnych rozwiązań w tym aspekcie?

1. System redundantny budowany jest w oparciu o **dokładnie te same moduły**, co system o architekturze Simplex. Nie ma zatem potrzeby inwestowania w inne rozwiązanie, dodatkowe licencje i kolejne technologie, które pozwolą podnieść dostępność naszego systemu. Wystarczy dodać redundantny kontroler i zainstalować moduły do synchronizacji danych.
2. System o architekturze redundantnej **konfiguruje się dokładnie tak samo**, jak system Simplex. Wykorzystujemy te same funkcje i procedury. Jedyne, co musimy zrobić dodatkowo, to wskazać obszary danych, które mają być synchronizowane między sobą.
3. System sterowania – bez względu na architekturę, w jakiej pracuje (czy Simplex, czy redundantnej) – zawsze jest dostępny dla aplikacji SCADA i systemów ▷

bazodanowych **pod jednym adresem IP**. To znacząco ułatwia podłączenie go do aplikacji wizualizacyjnych. Inżynierowie nie muszą wiedzieć, z którego kontrolera czytać dane – to system dba o to, aby dane zawsze były dostępne dla warstwy aplikacyjnej.

4. **Redundancji się nie programuje** – zajmują się tym wbudowane mechanizmy, które przygotowują konfigurację oraz wymieniają pomiędzy kontrolerami dane diagnostyczne i statusowe, niezbędne do oceny dostępności modułu rezerwowego. Programista nie musi się tym zajmować.
5. **Synchronizacja kontrolerów nie obciąża jednostki centralnej** i nie wpływa na cykl pracy kontrolera i jej wydajność. Dedykowane moduły do synchronizacji danych działają równolegle do procesora głównego i w każdym cyklu pracy dwa razy synchronizują dane między kontrolerami. Dzięki temu przełączenie na rezerwę może być zrealizowane w dowolnym momencie z gwarancją bezuderzeniowości.

Odporność na cyberataki

Cyberbezpieczeństwo – tego aspektu nie można pominąć, mówiąc o systemach z infrastruktury krytycznej. Budowa takich systemów często wykorzystuje architekturę rozproszoną, a więc siłą rzeczy **narażoną na potencjalne cyberataki** – z uwagi na konieczność komunikacji obiektów oddalonych między sobą.

Na bezpieczeństwo takich systemów mają wpływ zarówno ludzie, jak i wdrożone procesy, ale okazuje się, że aspekt ten nie jest obojętny także i dla producentów systemów automatyki. Wyposażają oni bowiem swoje układy w **dedykowane mechanizmy, które pozwalają podnieść bezpieczeństwo i odporność na cyberataki**. Musimy jednak pamiętać, że żaden system nie będzie w 100% bezpieczny, jeśli nie będziemy się stosować do rekomendowanych procedur bezpieczeństwa.

Emerson już od wielu lat wyposaża swoje produkty w rozwiązania, które chronią system przed nieuprawnionym dostępem, a z drugiej strony testuje urządzenia na nowe podatności i wdraża niezbędne poprawki i aktualizacje. Te – w postaci oficjalnych dokumentów – trafiają do użytkowników końcowych, którzy w oparciu o dostarczone materiały powinni zaktualizować oprogramowanie zgodnie z wytycznymi.

Na bezpieczeństwo takich systemów mają wpływ zarówno ludzie, jak i wdrożone procesy, ale okazuje się, że aspekt ten nie jest obojętny także i dla producentów systemów automatyki. Wyposażają oni bowiem swoje układy w ***dedykowane mechanizmy które pozwalają podnieść bezpieczeństwo i odporność na cyberataki****.*

Trusted Platform Module oraz **Secure Boot** to podstawowe mechanizmy wbudowane w każdą jednostkę centralną Emerson. W chwili jej uruchomienia przeprowadzana jest analiza, czy firmware i oprogramowanie systemowe mają niezbędne certyfikaty bezpieczeństwa i podpis cyfrowy, nadawany przez fabrykę. Inną funkcją uruchamianą w każdym kontrolerze jest wbudowany firewall, który wyłącza komunikację na portach, na których pojawia się nieuprawniony ruch. Dodatkowo możliwa jest weryfikacja uprawnień osób, które próbują się do kontrolera podłączyć. Testowany pod kątem konkretnych wektorów ataków kontroler oraz analiza jego podatności i odporności pozwalają nadać jednostkom centralnym Emerson **certyfikat Achilles Level 2**, który jest świadectwem odporności urządzeń na potencjalnie niebezpieczny ruch sieciowy.

Łatwa migracja ze starych do nowych urządzeń

Migracja to kolejny aspekt mający kluczowe znaczenie w aplikacjach klasyfikowanych jako krytyczne. W takich obiektach pełna wiedza na temat cyklu życia produktu, planowanych zmian w ofercie oraz wycofaniu towaru z obrotu ma dla użytkowników kluczowe znaczenie. W **Emerson każdy produkt ma aktualny status**, który jednoznacznie definiuje, w jaki sposób jest wspierany przez dostawcę i jak długo wspierany jeszcze będzie. Odpowiednio wcześniej pojawiają się informacje o planowanych zmianach w ofercie, dając użytkownikom czas na zaplanowanie właściwej ścieżki migracji.

Takie ścieżki i rekomendowane plany migracji Emerson dostarcza dla wszystkich swoich produktów, pokazując wprost, **jak zmienić jeden system na drugi** i w jakich kolejnych krokach należy to wykonać. Sama migracja jest zawsze wymagającym procesem, ale jeżeli jest dobrze zaplanowana, może być realizowana ze zminimalizowaniem ryzyka. Możliwość wykorzystania

posiadanych programów sterujących, modułów rozszerzeń, okablowania obiektowego, czy wręcz całych szaf sterujących to ważne korzyści dla użytkowników, którzy lata temu zainwestowali w urządzenia serii 90-30, a obecnie migrują je do serii PAC-Systems RX3i.

Dla użytkowników takich systemów ma to ogromne znaczenie. Zdejmuje bowiem bardzo dużo odpowiedzialności z inżynierów odpowiedzialnych za ten proces, ograniczając koszty i minimalizując czas niezbędny na przejście procesu.

System otwarty, z łatwą integracją z innymi urządzeniami

Z jednej strony bezpieczny, a z drugiej – otwarty? Czy tak się da? **Jeśli zastosujemy się do aktualnych standardów, jest to możliwe!** System, którego architekturę wymiany danych opieramy na globalnych standardach, pozwala łączyć między sobą różne urządzenia, pochodzące od różnych dostawców. W zależności od tego, na której warstwie systemu oczekujemy od niego otwartości, stosujemy dwa standardy komunikacji.

W warstwie I/O i urządzeń polowych powinniśmy postawić na PROFINET. Jest to szybka sieć przemysłowa, której standard nie jest własnością żadnego producenta automatyki. PROFINET pozwala łączyć ze sobą urządzenia różnych dostawców, zapewniając bardzo szybką wymianę danych – wystarczy zaimportować pliki GSDML do kontrolera, aby uruchomić komunikację z urządzeniem.

W Emerson standardem jest Gigabit PROFINET, co gwarantuje wymianę danych w czasie rzeczywistym nawet w bardzo rozbudowanych instalacjach. Sama sieć pozwala nie tylko na komunikację z urządzeniami, ale i na ich programowania poprzez sieć. PROFINET ma także jeszcze jedną bardzo istotną zaletę – może obsługiwać komunikację w topologii *Ring*, co czyni ją odporną na awarię lub rozłączenie dowolnego segmentu sieci. Pozwala na to wbudowana w kontroler sieci **obsługa Media Redundancy Protocol**, która w każdym kontrolerze Emerson jest standardem. Dzięki temu możemy budować system wysokiej dostępności na magistrali komunikacyjnej, nie inwestując dodatkowych środków.

W warstwie SCADA z kolei postawić należy na standard OPC-UA. To bardzo wydajny model komunikacji, pozwalający przesyłać duże ilości danych pomiędzy kontrolerem a systemami klasy SCADA bez względu na producenta, zastosowaną platformę sprzętową i system operacyjny, z jakiego korzystamy. OPC-UA ma jeszcze jedną istotną zaletę: posiada wbudowane mechanizmy zabezpieczeń w postaci haseł dostępu oraz certyfikatów, które muszą być skonfigurowane pomiędzy urządzeniami, które wymieniają dane. Na poziomie komunikacji pomiędzy warstwą sterującą a wizualizacyjną ma to kluczowe znaczenie dla zapewnienia bezpieczeństwa. To właśnie urządzenia pracujące na styku warstw są najbardziej narażone na potencjalny nieautoryzowany dostęp, dlatego należy dbać o to, aby komunikacja była realizowana w oparciu o niezależne interfejsy komunikacyjne, posiadające wbudowane mechanizmy zabezpieczeń.

Jakie ma to znaczenie dla systemów infrastruktury krytycznej? Ogromne. Nie inwestujemy w rozwiązania zamknięte, do których nie można podłączyć żadnych innych urządzeń. Mamy tym samym gwarancję, że w razie konieczności rozbudowy naszego systemu po prostu da się to zrobić. Co ważne: obsługa powyższych standardów jest w przypadku Emerson wbudowana w każdą jednostkę centralną, co nie wymusza na użytkowniku dodatkowych inwestycji.

Łatwy serwis i utrzymanie

Serwis i utrzymanie instalacji automatyki to kluczowy aspekt w obiektach infrastruktury krytycznej. To na służbach utrzymania ruchu oraz inżynierach procesu ciąży odpowiedzialność utrzymania instalacji w należytym stanie. Aby to było możliwe, **muszą mieć dostęp do aktualnych informacji**

diagnostycznych, dotyczących każdego obszaru działającego systemu. Poczynając od dostępu do tablic błędów logowanych w kontrolerze przez informacje diagnostyczne, udostępnianie przez poszczególne komponenty systemu sterowania, na monitorowaniu kanałów pomiarowych skończywszy.

Łatwy dostęp do tych danych oraz możliwość ich szybkiego pobrania i wysyłki do producenta, w celu weryfikacji i analizy potencjalnych przyczyn niewłaściwego zachowania, są dla inżynierów bardzo istotne. **W oprogramowaniu PAC Machine Edition diagnostyka pracy jest kluczowym elementem.** Może być dostępna w postaci:

- okna **Feedback Zone**, w którym programista na bieżąco widzi informacje dotyczące kompilacji aplikacji sterującej (otrzymując pełny raport o błędach i wyjątkach występujących na etapie kompilacji projektu),
- na poziomie programu sterującego w postaci bitów i słów statusowych, które mogą mieć wpływ na proces,
- raportów pracy kontrolera, wywoływanych na żądanie (w których znajduje się pełna specyfikacja projektowa, wykorzystanie dostępnych zasobów oraz informacja o wydajności),
- raportów generowanych przez narzędzia diagnostyczne, które mogą analizować parametry pracy urządzeń podłączonych na sieci PROFINET,
- narzędzi zewnętrznych, które zbierają dane z urządzeń polowych komunikujących się w oparciu o protokół Hart.

Przetwarzanie brzegowe

Dochodzimy do elementu, który w ramach czwartej rewolucji przemysłowej zaczyna odgrywać coraz większą rolę. Mowa tu o przetwarzaniu brzegowym. Idea podłączania urządzeń do chmury wydaje się stać w sprzeczności z systemami o znaczeniu krytycznym. W wielu przypadkach procedury wewnątrzzakładowe wręcz zabraniają podłączania urządzeń do sieci zewnętrznej, z uwagi na ryzyko nieuprawnionego dostępu. To słuszna strategia z punktu widzenia bezpieczeństwa, ale mocno ograniczająca korzyści, jakie daje możliwość przetwarzania danych w chmurze. Przykładem może tu być np. dostęp do zewnętrznych aplikacji, dających dodatkowe możliwości, takie jak analiza predykcyjna, kontekstowe udostępnianie informacji, projektowanie przepływów informacji i udostępnianie ich do służb utrzymania ruchu nowoczesnymi środkami komunikacji, dostęp do serwisów pogodowych, czy uczenie maszynowe.

> *Do szybkiego przetwarzania danych na poziomie produkcyjnym można wykorzystać **urządzenia do przetwarzania brzegowego**, przenosząc część funkcjonalności z chmury na lokalne urządzenia zainstalowane na poziomie produkcyjnym i odcięte od sieci zewnętrznej.*

Do szybkiego przetwarzania danych na poziomie produkcyjnym można wykorzystać **urządzenia do przetwarzania brzegowego**, przenosząc część funkcjonalności z chmury na lokalne urządzenia zainstalowane na poziomie produkcyjnym i odcięte od sieci zewnętrznej. Komunikujące się z kontrolerami procesowymi w oparciu o standard OPC-UA komputery brzegowe mają co prawda mniejszą wydajność w porównaniu z chmurą, ale dają dostęp do opisywanej wyżej funkcjonalności lokalnie. Wykonane w standardach przemysłowych pozwalają:

- uruchomić komunikację w oparciu standard MQTT i budować systemy IIoT, pozwalając na lokalne, bezprzewodowe oczujnikowanie maszyn w celu weryfikacji ich pracy oraz monitorowania odchyleń od normy (aby odpowiednio wcześniej ostrzegać o pracy poza standardowym zakresem pomiarowym),
- zamodelować proces przepływu informacji w oparciu o Node-Red pomiędzy urządzeniami oraz wykonywać konkretne akcje w związku z wystąpieniem konkretnej sytuacji (np. zapisać dane do lokalnej bazy danych, wysłać powiadomienie do właściwych odbiorców, wymusić uruchomienie konkretnej procedury),
- zwizualizować i w konkretnym kontekście przedstawić informacje różnym odbiorcom przy pomocy narzędzia Grafana (czy będą to informacje dotyczące zużycia energii dla energetyka, czy informacje o pojawiających się wibracjach dla służb utrzymania ruchu, czy dane o wydajności urządzenia, niezbędne dla managera produkcji),
- uruchomić lokalne systemy bazodanowe w celu składowania danych procesowych na wypadek utraty komunikacji z nadrzędnym systemem archiwizacji i przesłania danych do niego w chwili, gdy komunikacja zostanie przywrócona,
- uruchomić programy przygotowane w językach wysokiego poziomu (takich, jak Python), które mogą odwoływać się do zaprogramowanego modelu uczenia maszynowego w celu predykcji zachowań systemu i ostrzegania o możliwości wystąpienia potencjalnej awarii, zanim ona się wydarzy,
- przygotować serwisy WWW, które w oparciu o serwer Apache pozwolą udostępnić wybrane dane produkcyjne poza systemem automatyki (w postaci stron WWW),
- uruchomić lokalny firewall, na bieżąco filtrujący ruch sieciowy i blokujący połączenia, które mogą stanowić potencjalne zagrożenie i ryzyko dla aplikacji procesowej,
- uruchomić lokalne translatory protokołów, pozwalające zbudować w naszym systemie koncentrator danych pochodzących z różnych urządzeń obiektowych.

To zupełnie nowe funkcje, które powoli znajdują szersze zastosowania w układach automatyki. •

Infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje oraz usługi, kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (UZK)

Jak budować cyberbezpieczne aplikacje w oparciu o oprogramowanie AVEVA?

Jak projektować aplikacje, żeby spełniały wymogi cyberbezpieczeństwa w różnych aspektach? Jakie możliwości w tych kwestiach zapewnia Platforma Systemowa AVEVA? Poznaj przykładowe funkcjonalności, które pomagają budować bezpieczne systemy i dowiedz się, o czym przede wszystkim warto pamiętać.

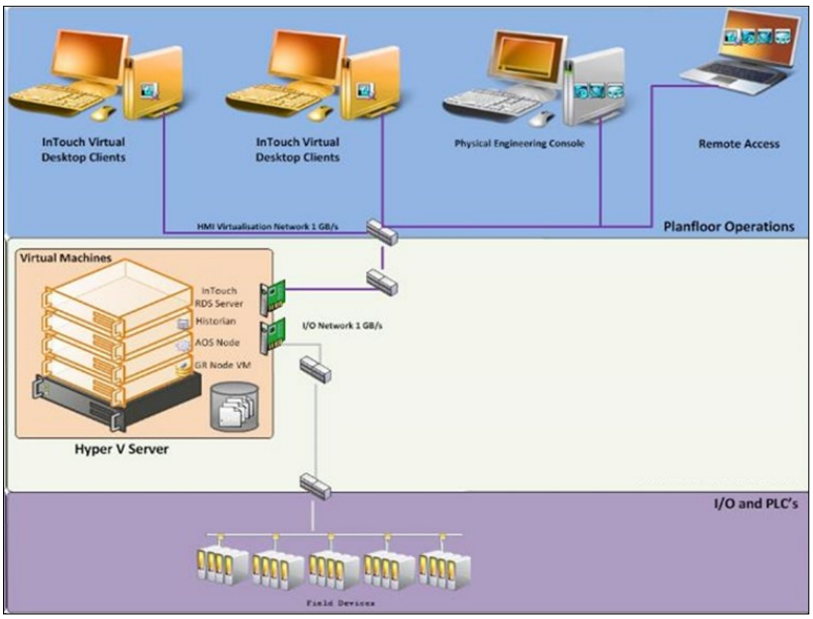
» Każda aplikacja projektowana w oparciu o system SCADA, zarówno na etapie tworzenia, jak i uruchamiania, wymaga dostępu z zewnątrz – albo z sieci biurowej, albo w ogóle spoza firmy. Dlatego też warto zadbać o odpowiednie zabezpieczenia na różnych poziomach. Szczególnie konieczne jest zapewnienie bezpiecznego dostępu sieciowego, zachowania ciągłości pracy oraz dostępu do danych.

Bezpieczny dostęp sieciowy

Pierwszym krokiem jest **zabezpieczenie sieci na brzegach**. Oznacza to, że nikt spoza zakładu nie powinien móc się dostać do sieci zakładowej w sposób niekontrolowany. W tym celu możemy wykorzystać narzędzia **firewall** oraz **NG firewall** (Next Generation Firewall), które umożliwiają zabezpieczenie dostępu do sieci poprzez narzucenie ograniczeń na poszczególne porty i protokoły komunikacyjne. W przeciwieństwie do zwykłego firewalla, NG firewall dodatkowo analizuje ramki, ich kształt oraz sygnatury ruchu, które przepływają przez sieć – i pozwala na ograniczanie dostępu również na ich podstawie.

Do skonfigurowania zabezpieczenia wewnątrz sieci zakładowej wykorzystywany jest Windows Firewall – standardowe narzędzie dostępne w każdej wersji systemu Microsoft Windows. Nie wymaga ono specjalnej konfiguracji – instalator oprogramowania AVEVA sam otwiera porty, które są potrzebne.

W przypadku komputerów wewnątrz sieci często potrzebny jest dostęp zdalny. Może on przyjmować dwie formy, w zależności od sytuacji. **Gdy potrzebujemy komunikacji dwukierunkowej** (np. dwie części firmy znajdują się w różnych lokalizacjach i musimy wymieniać między nimi informacje) dobrym rozwiązaniem jest **VPN Site-2-Site**, który daje możliwość dwukierunkowej wymiany danych. Natomiast **kiedy chcemy podłączyć zdalnego użytkownika** (np. inżyniera projektującego, który będzie wykonywać pewne zadania na naszej aplikacji), idealnym rozwiązaniem jest **VPN klient-serwer**.



Rys. 1. Aplikacja przemysłowa w środowisku zwirtualizowanym. Źródło: AVEVA

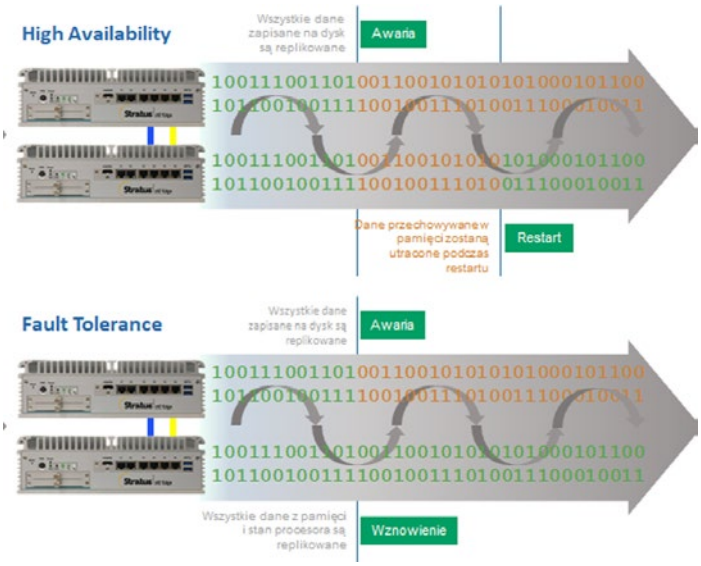
Na jakiej infrastrukturze stawiać aplikację?

Najczęściej wybieraną opcją jest infrastruktura własna (On-Premise). W przypadku budowania i utrzymania serwerów fizycznych warto zadbać o **moduły zarządzania zdalnego** (iDRAC – DELL oraz iLO – HP), dzięki którym można zarządzać komputerami z każdego miejsca (konfiguracja, restarty). Ważne jest, aby aktualizować moduły zarządzania w celu zapewnienia bezpieczeństwa oraz stabilności.

Sporo możliwości daje budowanie systemu na środowiskach **zwirtualizowanych**. W tym wypadku AVEVA zdecydowała się wspierać rozwiązania **VMWare vSphere** oraz **Microsoft Hyper-V**. Pozwala to uzyskiwać systemy wysokiej dostępności. Dużym plusem jest tutaj niezależność od sprzętu – wirtualne maszyny można przenosić między jednym serwerem a drugim (np. w przypadku awarii możemy przenieść całe, już działające, skonfigurowane systemy na inny serwer).

Również w przypadku Hyper-V i VMWare nie można zapominać o koniecznych aktualizacjach.

Autor: **Marcin Woźniczka**
Starszy specjalista ds. oprogramowania przemysłowego, ASTOR
marcin.wozniczka@astor.com.pl



Rys. 2. Porównanie poziomów ochrony High Availability i Fault Tolerance. Źródło: ASTOR

Trzeba regularnie sprawdzać, czy oprogramowanie SCADA wspiera wersje produktów, który zakupiliśmy i chcemy używać w tych środowiskach. Choć może się to wydawać oczywiste, warto wspomnieć też o konieczności zabezpieczania aplikacji poprzez systemy kopii zapasowych. Powinno się je tworzyć regularnie, w sposób automatyczny – dzięki temu można zawsze wrócić do jakiegoś wcześniejszego punktu.

Ciekawe możliwości otwiera również zastosowanie **systemów typu Shadow, inaczej zwanych Pre-Prod**. Są to wirtualne kopie systemu produkcyjnego, ale w wersji nieprodukcyjnej – swego rodzaju bliźniacze aplikacje, na których można wykonywać próbne migracje czy aktualizacje, a także duże zmiany w działaniu systemu. Pozwala to przeprowadzać testy bez ryzyka ewentualnej awarii czy wystąpienia innego problemu w systemie produkcyjnym.

Jak zapewniać ciągłość pracy?

Ciągłość pracy można zapewnić w oparciu klastry wysokiej dostępności, bazujące na serwerach, macierzach dyskowych oraz na specjalizowanych licencjach. Generuje to jednak duże koszty, a stworzenie takiego układu i jego skonfigurowanie wymaga sporej wiedzy z zakresu IT.

Alternatywą jest wykorzystanie **funkcjonalności redundancji w oprogramowaniu przemysłowym**. Silniki aplikacyjne w Platformie Systemowej AVEVA mają możliwość pracy w parach. Dzięki temu w przypadku awarii komputera, na którym działa pierwszy silnik i jego logika, nastąpi przełączenie umożliwiające dalszą pracę oprogramowania na drugim komputerze z rezerwowym silnikiem aplikacyjnym. Podobnie możliwości dostępne są również w przypadku oprogramowania Historian, a także w zakresie redundancji torów komunikacyjnych.

Istnieje też trzecia opcja – zapewnienie ciągłości pracy w oparciu o **rozwiązanie firmy Stratus ztc Edge**, czyli wykorzystanie dwóch komputerów przemysłowych, które mają wbudowaną wirtualizację. Jest to autorskie rozwiązanie systemu wysokiej dostępności firmy Stratus do wirtualizacji, przeznaczone dla automatyków. Mimo, że nie jest oparte na VMWare vSphere czy Microsoft Hyper-V, jest ono wspierane przez AVEVA, więc można je stosować z Platformą Systemową oraz oprogramowaniem InTouch i Historian.

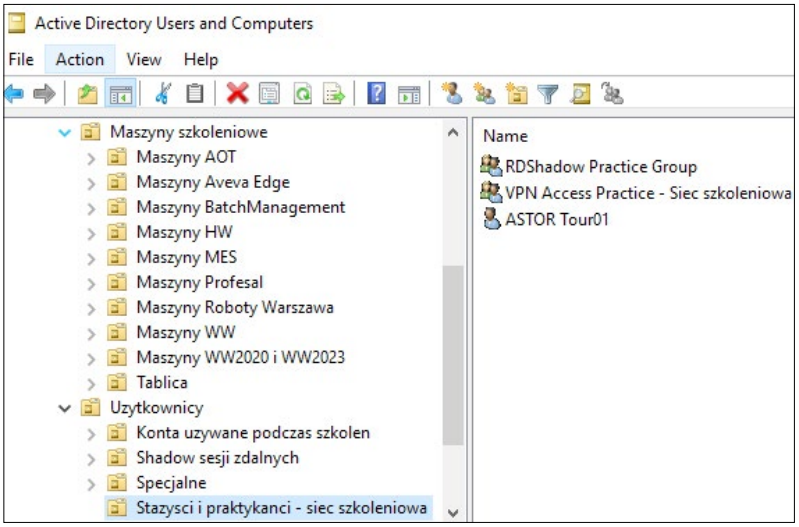
Rozwiązanie to ma wiele istotnych zalet:

- nie wymaga ono zaawansowanej wiedzy IT,
- zarządzanie systemem jest łatwe (za pośrednictwem aplikacji webowej),
- wbudowana zapora chroni przed ewentualnymi atakami z zewnątrz,
- można je zainstalować w szafie sterowniczej, na szynie DIN,
- dostępny jest szeroki wybór poziomu ochrony HA (High Availability) lub FT (Fault Tolerant),
- Hot-Swap – w przypadku awarii jednego komputera można wymienić go na zapasowy „na ruchu”,
- udostępniane są regularne aktualizacje oprogramowania, związane z zarządzaniem komputerami pod kątem ryzyka i zagrożeń bezpieczeństwa.

Systemy operacyjne

Aby zapewnić bezpieczeństwo systemów operacyjnych, trzeba zwracać uwagę, czy używane przez nas wersje oprogramowania są aktualne, a producent wciąż weryfikuje i testuje swoje produkty z tymi systemami. Przykładowo Microsoft przestał już wspierać niektóre wersje Windowsa 10. Podobnie jest w przypadku starych wersji produktów AVEVA. Każda wersja oprogramowania ma status wsparcia przez określony czas od pojawienia się na rynku. Żeby mieć pewność, że korzystamy z oprogramowania w wersji bezpiecznej, trzeba regularnie je aktualizować.

AVEVA testuje aktualizacje systemowe Microsoftu pod względem kompatybilności ze swoim oprogramowaniem i do 15 dni od ich publikacji udostępnia raport z ich kompatybilności. Dobrą praktyką jest więc aktualizacja systemu już udostępnieniu tego raportu. Najlepiej robić to za pomocą własnego serwera WSUS, czyli lokalnego serwera aktualizacji Windows. Dzięki temu w pełni kontrolujemy, kiedy i jakie aktualizacje są instalowane.

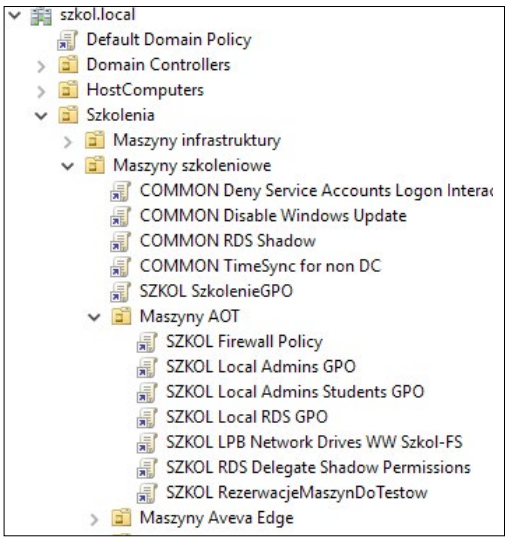


Rys. 3. Konfiguracja Active Directory. Źródło: ASTOR

Dostęp do danych, poświadczenia i uprawnienia użytkowników

Żeby efektywnie zarządzać poświadczeniami i uprawnieniami użytkowników, najlepiej stosować **Active Directory**, czyli system zarządzania domeną firmy Microsoft. Dobrze, gdyby domena przeznaczona do obsługi oprogramowania przemysłowego była oddzielona od domen korporacyjnych czy ogólnozakładowych. Zastosowanie domeny pozwala konfigurować uprawnienia użytkowników za pomocą systemu ról. Dla każdej utworzonej roli przypisujemy odpowiedni poziom uprawnień, a następnie poszczególnym użytkownikom przypisujemy właściwe role. Dzięki temu centralnie zarządzamy wszystkimi uprawnieniami dostępu.

Zastosowanie domeny pozwala także centralnie zarządzać innymi elementami zabezpieczeń, np. możemy definiować wspólne reguły zapory

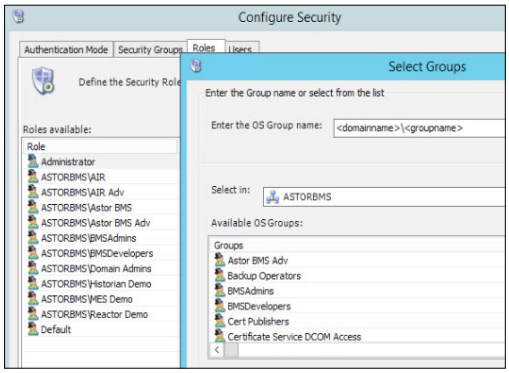


Rys. 4. Konfiguracja Active Directory. Źródło: ASTOR

ogniowej Windows, zasady zabezpieczeń lokalnych czy wspólne ustawienia identyczne dla wszystkich komputerów w sieci.

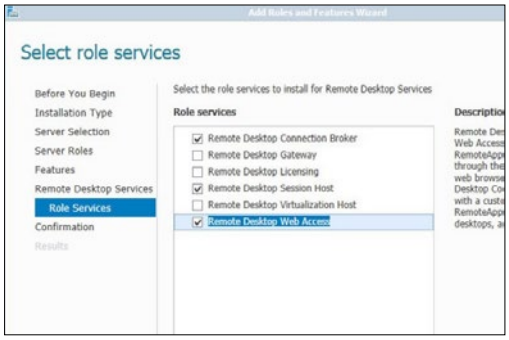
W Active Directory można tworzyć grupowe konfiguracje. Dzięki temu wystarczy dodać komputer do danej grupy, a ustawione polityki czy konfiguracje automatycznie są na nim aplikowane, bez potrzeby indywidualnej konfiguracji.

Plusem jest też możliwość integracji z systemem SCADA. Aplikacje Platformy Systemowej AVEVA można konfigurować w taki sposób, że role w systemie SCADA będą powiązane z rolami w Active Directory. Dzięki temu wystarczy tylko raz dodać danego użytkownika na poziomie Active Directory i od razu mamy pewność, że otrzymał on swoją właściwą rolę także w systemie SCADA.



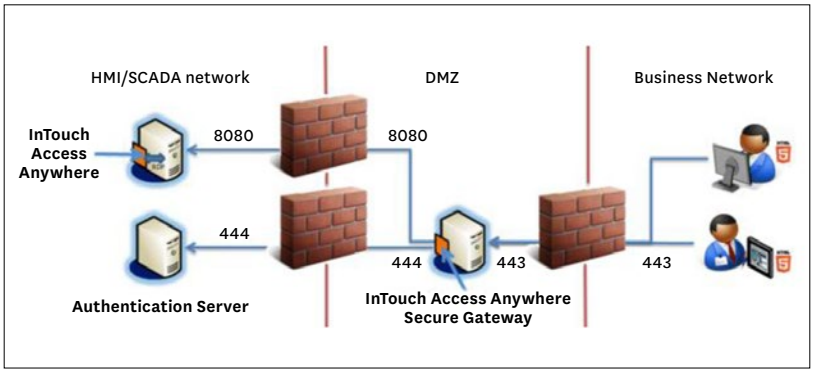
Rys. 5. Konfiguracja ról dla użytkowników. Źródło: ASTOR

Domena jest też potrzebna podczas budowania środowiska terminalowego zdalnego dostępu RDS (Remote Desktop Services). AVEVA zaleca, by stosować ją również w przypadku używania np. AVEVA Batch Management czy AVEVA MES.



Rys. 6. Konfiguracja ról dla użytkowników. Źródło: ASTOR

Dodatkowo Active Directory pozwala sterować uprawnieniami użytkowników włączających się do sieci z zewnątrz, czyli na przykład po WiFi albo przez VPN. Dzięki domenie mamy więc pełną kontrolę nad naszym systemem. ▷



Rys. 7. InTouch Access Anywhere Secured Gateway. Źródło: ASTOR

Cyberbezpieczeństwo w AVEVA

AVEVA nieustannie udoskonala swoje produkty w zakresie cyberbezpieczeństwa. Regularnie przeprowadzane są różnego rodzaju testy, które mają zapobiegać powstawaniu luk bezpieczeństwa już na poziomie kodu źródłowego. Weryfikowane są również komponenty, które były stworzone wiele lat temu – jeżeli pojawiają się jakieś nieprawidłowości, w kolejnych wersjach AVEVA wprowadza poprawki niwelujące lub minimalizujące zagrożenia.

AVEVA stawia przede wszystkim na wiedzę ludzi, którzy tworzą oprogramowanie. W oparciu o procedury SDLA (*Security Development Lifecycle Assurance)* wszyscy programiści AVEVA przechodzą szkolenia, przygotowujące do projektowania cyberbezpiecznych aplikacji.

Dla produktów znajdujących się w głównej fazie wsparcia (zazwyczaj do 3 lat od wypuszczenia na rynek) AVEVA na bieżąco testuje poprawki Microsoftu weryfikując, czy ich instalacja nie wpływa negatywnie na działanie aplikacji AVEVA. Zazwyczaj są one przetestowane w ciągu 15 dni roboczych od momentu wypuszczenia przez Microsoft. Użytkownicy mogą sprawdzać wyniki tych testów na udostępnianym przez AVEVA portalu Security Central. Aby być na bieżąco z zaleceniami i aktualnymi testami, warto też zasubskrybować Biuletyn Bezpieczeństwa i alerty techniczne wysyłane przez AVEVA. Zawierają one istotne informacje na temat potencjalnych zagrożeń.

Jakie mechanizmy w oprogramowaniu AVEVA ułatwiają tworzenie cyberbezpiecznych aplikacji?

W Platformie Systemowej AVEVA, począwszy od wersji 2017, wspierany jest **TLS 1.2**, a sama Platforma Systemowa oraz oprogramowanie InTouch umożliwiają włączenie szyfrowania komunikacji. Wskazując odpowiedni certyfikat, generowany automatycznie lub dostarczany przez dział IT, możemy zapewnić szyfrowanie danych przekazywanych między komponentami naszej aplikacji.

Nowoczesne systemy SCADA często wymagają, aby pracownicy mieli zdalny dostęp do wizualizacji spoza firmy, z poziomu przeglądarki internetowej. Aby w sposób bezpieczny uruchomić taki dostęp, możemy posłużyć się modułem **InTouch Access Anywhere.** Jest to rozwiązanie, które doskonale sprawdza się w przypadku użytkownika, który sporadycznie potrzebuje skorzystać z aplikacji InTouch poza firmą i bez zainstalowanego programowania AVEVA.

Żeby taki dostęp był bezpieczny, możemy skonfigurować w strefie DMZ komponent o nazwie **InTouch Access Anywhere Secured Gateway**. Pośredniczy on w wymianie danych umożliwiając jej szyfrowanie (HTTPS) oraz izoluje klienta webowego od wewnętrznej sieci przemysłowej, czyniąc ją bezpieczniejszą. Funkcjonalność ta nie wymaga dodatkowej licencji.

W przypadku konieczności podłączenia się do wizualizacji przez przeglądarkę internetową (również z komórki lub tabletu), możemy skorzystać z **natywnego dostępu webowego do InToucha** (InTouch Web Client). W tym przypadku mamy kilka opcji zabezpieczenia do wyboru, m.in. opcję szyfrowania danych z wykorzystaniem protokołu HTTPS lub HTTPS z AIM, czyli **AVEVA Identity Manager**, który umożliwia autoryzację użytkownika spoza firmy.

Począwszy od wersji 2023 Platformy Systemowej AVEVA można też skorzystać z Active Directory działającego w chmurze **Microsoft Azure**. Dzięki temu nie ma potrzeby konfigurowania Active Directory we własnej sieci. Bonusem jest też możliwość logowania się do systemu za pomocą webowego okna logowania z możliwością włączenia dwuetapowej weryfikacji kont.

Podsumowanie

Wśród dobrych praktyk związanych z projektowaniem cyberbezpiecznych aplikacji do najważniejszych należą regularne aktualizacje. Produkty AVEVA nie tylko oferują wiele funkcjonalności wspomagających tworzenie bezpiecznych rozwiązań, ale przede wszystkim są na bieżąco udoskonalane i uaktualniane.

Jeśli chcesz dowiedzieć się więcej na temat stosowanych przez AVEVA procedur wspierających cyberbezpieczeństwo – skontaktuj się z nami. •

Transport hybrydowy w zasięgu ręki

End of line z użyciem robotów mobilnych (AMR)

Końcówki linii produkcyjnych mogą wydawać się mniej istotnymi elementami procesu produkcyjnego. Gdy myślimy o automatyzacji lub optymalizacji produkcji, zwykle staje nam przed oczami zasadnicza część tego procesu: maszyny i technologia. Końcówka pozornie jest banalna – cóż, produkt na końcu trzeba spakować i wysłać do magazynu. Tymczasem to „pakowanie i wysłanie do magazynu" jest niezwykle istotne – i może znacząco wpływać na efektywność całej produkcji oraz jakość wyrobu końcowego.

AUTOR: **Kinga Tarsa**
Koordynator marketingu w Linii Biznesowej Intralogistyka
kinga.tarsa@astor.com.pl

» Końcówka linii to właśnie ten ostatni etap. Składają się na nią: paletyzacja, owijanie, bandowanie / wiązanie, etykietowanie, ważenie oraz transport do magazynu końcowego – przy czym warto pamiętać, że w konkretnych systemach nie wszystkie te elementy muszą zawsze występować. W klasycznej, niezautomatyzowanej produkcji etap ten odbywa się zwykle z bardzo dużym udziałem ludzi. Produkty są ręcznie układane na paletach, a te są transportowane wózkami paletowymi ręcznymi, widłowymi czołowymi lub bocznymi. Zarówno owijanie folią, jak i etykietowanie wykonywane są również ręcznie. Wiąże się to jednak z kilkoma wyzwaniami.

Po pierwsze proces odbywa się z dużym udziałem ludzi. Tymczasem dziś firmy często borykają się z brakiem pracowników lub ich dużą rotacją, są więc zmuszone posiłkować się pracownikami krótkoterminowymi zatrudnianymi przez zewnętrzna firmę. Praca na końcówce linii jest ciężka, monotonna, a bywa też niebezpieczna. Wystarczy niewielki błąd lub niedokładność, a pojawić się może poważne zagrożenie dla operatora. Dodatkowo zyski firmy pomniejsza wciąż rosnący koszt surowców używanych do pakowania, a także konieczność redukcji liczby reklamacji i zwrotów.

Istotny udział czynnika ludzkiego sprawia też, że trudno o uzyskanie wysokiej wydajności i powtarzalności w procesie paletyzowania czy etykietowania. W takim przypadku najczęściej szybko okazuje się, że nasza końcówka linii staje się wąskim gardłem dla całego procesu, który jest zautomatyzowany i wydajny. Cała poprawa efektywności i oszczędności uzyskane na wcześniejszych etapach produkcji są zaprzepaszczane na samym końcu.

Automatyzacja procesu umożliwia także zachowanie jednakowej, wysokiej jakości, co przekłada się na mniejszą liczbę reklamacji. Innym efektem jest także mniejsze zużycie materiałów. Przykładowo automatyczna owijarka regulując naciąg folii pozwala na zmniejszenie ilości folii użytej na pojedynczą paletę.

Automatyzacja transportu

Antidotum na te problemy jest zautomatyzowany i zrobotyzowany system paletyzacji i transportu wyrobów gotowych. Może on stanowić połączenie klasycznego rolkowego, łańcuchowego lub taśmowego transportu produktów/palet z robotami paletyzującymi oraz mobilnymi robotami transportującymi produkt końcowy do magazynu. W takim systemie:

- robot układa wyroby na paletach,
- palety są transportowane automatycznie za pomocą klasycznego systemu rolkowego / łańcuchowego / taśmowego i/lub robota mobilnego (AMR),
- palety są owijane w automatycznych owijarkach talerzowych, ramieniowych i/lub pierścieniowych,
- zautomatyzowany jest również proces etykietowania i weryfikacji etykiety,
- roboty mobilne odwożą gotowe palety do magazynu.

Rozwiązanie takie może być również całkowicie zintegrowane z nadrzędnym systemem zarządzania produkcją, co umożliwia automatyczne śledzenie całego zlecenia produkcyjnego od jego wygenerowania aż do umieszczenia gotowego wyrobu w magazynie.

Elementy składowe systemu

Zautomatyzowany system paletyzacji i transportu na końcówce linii produkcyjnej składa się zwykle z:

- robota paletyzującego z chwytakiem,
- systemu transporterów wraz z owijarką i etykieciarką,
- zderzaków mechanicznych palet,
- robota AMR z nożycowym mechanizmem podnoszenia palet,
- systemu informatycznego umożliwiającego obsługę zleceń generowanych i przesłanych przez system MES.

Opcjonalnie system można wyposażyć w:
- magazynek palet,
- magazynek przekładek.

System realizuje następujące funkcje technologiczne:
- odbiór palet z gniazd automatycznej paletyzacji oraz ręcznej paletyzacji,
- automatyczne podawanie palet z gniazd paletyzacji na ciąg transportowy,
- automatyczne buforowanie palet,
- automatyczne owijanie palet folią oraz krycie górne,
- automatyczne etykietowanie palet z jednej strony, lub dwóch stron: przód oraz bok, lub przód oraz tył,
- automatyczne skanowanie ostatniego kodu etykiety, umożliwiające potwierdzenie poprawności procesu etykietowania.

Oprogramowanie natomiast realizuje funkcje obsługi przesłanego zlecenia:
- odbiór zlecenia produkcyjnego,
- wybór odpowiedniego programu owijania, zależnego od produktu,
- etykietowanie z wykorzystaniem umieszczonych w zleceniu danych,
- weryfikacja etykietowania za pomocą umieszczonego na ramieniu etykieciarki skanera,
- przesłanie informacji o umieszczeniu palety w magazynie do systemu nadrzędnego.

Przykładowe systemy

Poniżej przedstawiamy wizualizacje dwóch przykładowych systemów.

Pierwszy z nich to proste rozwiązanie, pozwalające zrobotyzować proces paletyzacji. Stanowisko składa się z jednego przenośnika doprowadzającego produkt w strefę pracy robota. Robot przy użyciu chwytaka układa produkt na palecie zgodnie z zaprogramowanym schematem paletyzacji. Dodatkowo robot ma możliwość układania przekładek pomiędzy warstwami produktów. Stanowisko obejmuje dwa pola odkładcze (palety) do paletyzacji produktu oraz jedną paletę z przekładkami. Dostawa przekładek do stanowiska, transport pustych palet oraz odbiór pełnych jest wykonywana przez robota mobilnego AMR – Agilox ONE.

↳ https://www.youtube.com/watch?v=hmbq1VmQang

Drugi przykład to stanowisko wyposażone w jeden przenośnik doprowadzający produkt w strefę pracy robota. Robot przy użyciu chwytaka układa produkt na palecie zgodnie z zaprogramowanym schematem paletyzacji. Dodatkowo robot ma możliwość układania przekładek pomiędzy warstwami produktów. Rozwiązanie jest rozbudowane o magazynek palet, który pozwala automatycznie dostarczać palety w pole odkładcze robota. Dzięki temu wzrasta wydajność – robot paletyzujący nie musi pobierać palety i odkładać jej na wyznaczone miejsce. Transport gotowej palety, jak i przekładek do stanowiska wykonuje robot mobilny AMR – MiR 600.

↳ https://www.youtube.com/watch?v=1ZL_7rS0K38

Co zyskujemy?

Zautomatyzowany system paletyzacji i transportu na końcówce linii produkcyjnej przynosi wymierne korzyści. Wśród najważniejszych można wymienić:
- Znaczące zwiększenie wydajności systemu w stosunku do rozwiązania opartego na pracy ręcznej.
- Zapewnienie stałej i przewidywalnej wydajności – system może pracować bez przerw przez 24 godziny na dobę i 7 dni w tygodniu.
- Zagwarantowanie bezpieczeństwa w procesie paletyzacji i transportu zarówno dla operatorów, jak i dla Utrzymania Ruchu,
- Zapewnienie zbilansowanego czasu poszczególnych operacji w procesie produkcyjnym, co przekłada się na płynne działanie systemu.
- Zmniejszenie liczby zwrotów i reklamacji.
- Zapewnienie stałej jakości owijania i etykietowania.
- Redukcja ryzyka związanego z absencją i rotacją pracowników.
- Zwiększenie elastyczności systemu, który łatwiej może być dostosowywany do zmieniających się potrzeb. •

Wysokowydajne sterowniki PLC Astraada One Modular oparte na Raspberry Pi®

Raspberry Pi®, mimo że pierwotnie nie był projektowany dla sektora przemysłowego, zdobył uznanie jako minikomputer doskonale sprawdzający się w tym obszarze. W dobie koncepcji Przemysłu 4.0 zapotrzebowanie na moc obliczeniową przekracza możliwości konwencjonalnych rozwiązań, stąd też wiele innowacyjnych firm decyduje się na wykorzystanie minikomputerów, wspierając tym samym transformację technologiczną i cyfryzację procesów produkcyjnych.

» **Astraada One** to seria wydajnych sterowników, które swoimi możliwościami sięgają poza standardowy zakres możliwości PLC. Wychodzą one naprzeciw wymaganiom nowoczesnych systemów sterowania, łącząc zaawansowane funkcjonalności z prostotą programowania. Sterowniki z rodziny Astraada One sprawdzają się świetnie w małych i średnich instalacjach.

Sterowniki **Astraada One** dostępne są w trzech wersjach obudowy – modułowej (**One Modular**), kompaktowej (**One Compact**), kompaktowej z wbudowanym panelem HMI (**One Compact HMI**), a także w postaci prostego terminala operatorskiego (**One Terminal**). Niezależnie od wariantu obudowy wszystkie modele programowane są w niezależnym i bezpłatnym środowisku **CODESYS**.

Rodzinę sterowników Astraada One uzupełnia modułowy sterownik bezpieczeństwa **Astraada One Safety**, w ramach którego dostępna jest jednostka centralna oraz układy rozszerzeń wejść/wyjść. Sterownik bezpieczeństwa działa jako urządzenie *slave* jednostki głównej Astraada One, dzięki czemu program bezpieczeństwa można zawrzeć w tym samym projekcie CODESYS, co główny program sterujący.

Astraada One Modular – wydajne i elastyczne sterowniki PLC

Seria modułowych sterowników programowalnych rodziny Astraada One to rozwiązanie przeznaczone do sterowania małymi i średnimi aplikacjami automatyki przemysłowej, jak również bardziej rozbudowanymi, wymagającymi obsługi wielowątkowej.

Projektant ma pełną dowolność konfiguracji wejść/wyjść, portów komunikacyjnych i funkcjonalności sterownika. Moduły komunikują się wzajemnie za pośrednictwem protokołu EtherCAT, dzięki czemu wymiana danych przebiega szybko i bez zakłóceń. Seria Modular zawiera zróżnicowany wybór jednostek, dzięki czemu sterownik można dostosować do potrzeb. Dzięki wykorzystaniu dedykowanych modułów istnieje możliwość budowania oddalonych układów wejść/wyjść oraz systemów bezpieczeństwa.

Nowe jednostki centralne Astraada One Modular oparte są na platformie Raspberry Pi. Wyposażone są w bardzo wydajne procesory czterordzeniowe, w których każdy rdzeń taktowany jest z częstotliwością 1,5GHz, co umożliwia przetwarzanie wielowątkowe przy czasach cyklu sięgających 500 µs. Obsługują nawet do 8 GB pamięci flash. Całość montowana jest na szynie DIN, a wymianę danych zapewnia wewnętrzna magistrala EtherCAT.

W ramach rodziny Astraada One Modular dostępne są trzy modele jednostki centralnej: Pi-Pro, Pi-Prime oraz Pi-Plus.

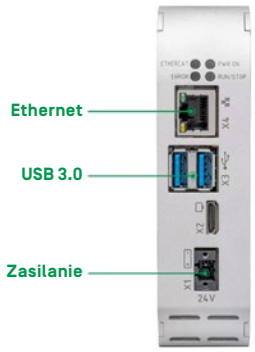
AUTOR: **Mateusz Pytel**
Menedżer produktu Astraada One
mateusz.pytel@astor.com.pl

Astraada One Modular Pi-Pro

Imponuje doskonałą wydajnością w czasie rzeczywistym dzięki czterordzeniowemu procesorowi, bazującym na najnowszej technologii Raspberry Pi, a także doskonale skoordynowanemu sprzętowi i oprogramowaniu.

Rodzina jednostek centralnych Astraada One Modular. Źródło: ASTOR

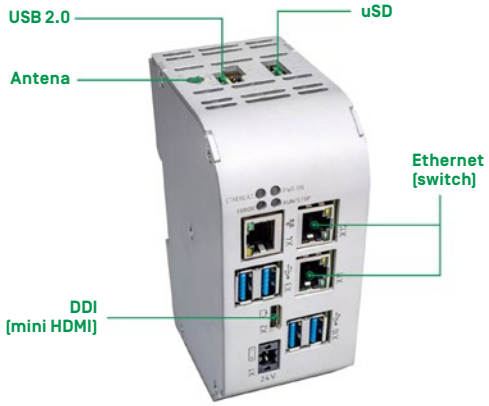
Najważniejsze parametry:
- CPU 1,5 GHz Quad Core
- 1 GB RAM / 8 GB Flash / 100 kB Retain
- 2× Host USB 3.0
- 1× EtherCAT LVDS
- 1× Ethernet
- 1× DDI (mini HDMI)



Astraada One Modular Pi-Pro. Źródło: ASTOR

Astraada One Modular Pi-Prime

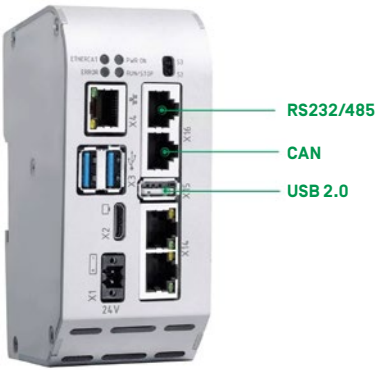
Ta jednostka posiada dwukrotnie więcej pamięci nieulotnej, ważnej dla podtrzymania programu przy zaniku zasilania. Posiada również dodatkowo 2-portowy switch Ethernet oraz gniazdo karty µSD, ułatwiające modyfikowanie, wgrywanie lub tworzenie kopii zapasowej na karcie SD sterownika PLC.
Najważniejsze parametry:
- CPU 1,5 GHz Quad Core
- 1 GB RAM / 8 GB Flash / 200 kB Retain
- 4× Host USB 3.0
- 1× EtherCAT LVDS
- 1× Ethernet
- 1× DDI (mini HDMI)
- 1× Ethernet 2-port switch
- 1× µSD



Astraada One Modular Pi-Prime. Źródło: ASTOR

Astraada One Modular Pi-Plus

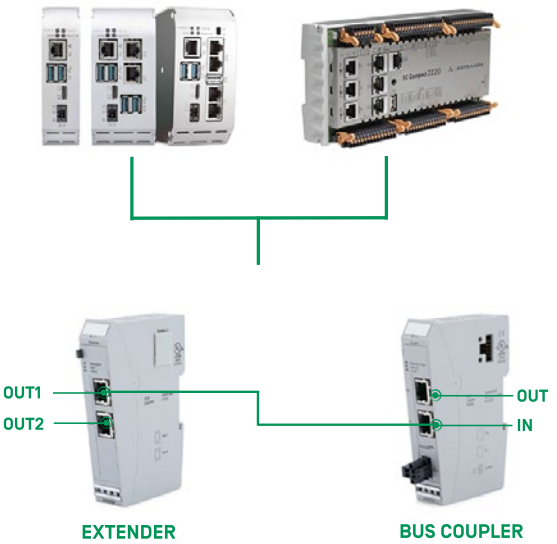
Najwyższy model zapewnia obsługę komunikacji szeregowej w standardach RS232/RS485 oraz CAN, dzięki czemu idealnie nadaje się do obsługi zadań bazujących na Softmotion CNC, umożliwiając m.in. synchronizację napędów czy obsługę G-CODE.
Najważniejsze parametry:
- CPU 1,5 GHz Quad Core
- 1 GB RAM / 8 GB Flash / 200 kB Retain
- 3× Host USB 3.0
- 1× EtherCAT LVDS
- 1× Ethernet
- 1× DDI (mini HDMI)
- 1× Ethernet 2-port switch
- 1× uSD
- 1× RS232/RS485
- 1× CAN



Astraada One Modular Pi-Plus. Źródło: ASTOR

Budowa systemu w oparciu o Astraada One

Podstawowym elementem każdego układu opartego na modułowym sterowniku Astraada One jest jednostka centralna z rodziny MC-Pi. Do tego modułu możemy, w zależności od potrzeb, dołączać dodatkowe moduły I/O. Dzięki wykorzystaniu modułów Buscoupler oraz Extender Port mamy możliwość zbudowania rozproszonych układów wejść/wyjść. Rodzinę Astraada One Modular możemy dowolnie powiększać o kolejne moduły rozszerzeń jak również moduły kompaktowe.



Budowa systemu rozproszonego opartego na Astraada One Modular. Źródło: ASTOR

Przy tworzeniu modułowej architektury sterowania należy pamiętać o pewnych zasadach:
- do jednostki centralnej można podłączyć maks. 10 modułów (do dalszej rozbudowy wymagany jest moduł Extender Port),
- do modułu Buscoupler można podłączyć maks. 20 modułów.

Astraada One Modular Safety

Innowacyjne i zintegrowane rozwiązanie systemu bezpieczeństwa obejmuje swobodnie programowalny PLC SC-1000 oraz moduł SC-I/O zgodne z wymaganiami norm bezpieczeństwa IEC 61508 SIL 3 i DIN ISO 13849-1 PLe.

Rdzeń SC-1000 to dwa mikroprocesory, które realizują funkcje bezpieczeństwa i komunikują się ze sobą w celu wymiany danych procesowych i wzajemnego monitorowania. Trzeci mikroprocesor zarządza komunikacją zewnętrzną.

Moduł Safety I/O posiada 4 wejścia cyfrowe i 2 wyjścia cyfrowe oraz umożliwia podłączenie powszechnie stosowanych urządzeń bezpieczeństwa. Wyjścia modułu zapewniają bezpieczne podłączenie elementów wykonawczych, takich jak styczniki, kontrolki lub napędy. Jako standardowe moduły dodatkowe ze zintegrowanym systemem magistralnym, urządzenia te można łatwo zainstalować i połączyć z innymi komponentami sterującymi.

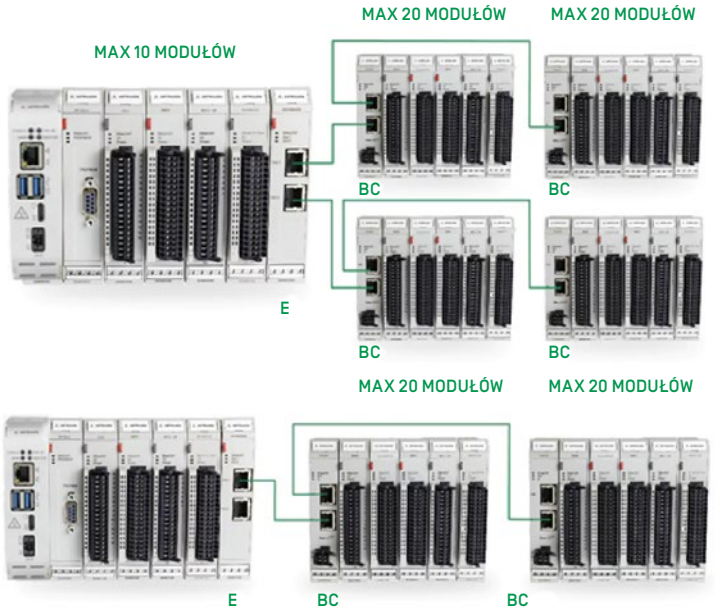
Cechy urządzenia:

- Komunikacja Failsafe over EtherCAT (FSoE).
- Standardy bezpieczeństwa IEC 61508 SIL 3 i DIN EN ISO 13849-1 PL e.
- Możliwość rozbudowy o moduły bezpiecznych wyjść oraz wejść dyskretnych.
- Wymaga sterownika nadrzędnego Astraada One.
- Montaż na szynę DIN.
- Możliwość rozproszenia układu bezpieczeństwa na inne wyspy I/O Astraada One Modular.

Korzyści wynikające ze stosowania sterownika bezpieczeństwa:

- Elastyczność realizowania funkcji bezpieczeństwa maszynowego poprzez możliwość pracy w jednym, otwartym środowisku programistycznym CODESYS, bez żadnych dodatkowych deweloperskich nakładek.
- Łatwość rekonfiguracji i diagnostyki, przy jednoczesnym zabezpieczeniu przed nieautoryzowanymi zmianami w programie bezpieczeństwa. W razie potencjalnej awarii, oprócz zapewnienia bezpieczeństwa, można łatwo zlokalizować i naprawić źródło usterki, dzięki czemu minimalizujemy czas przestoju oraz zwiększamy czas eksploatacji maszyn.
- Oddalone układy I/O – wyróżniające rozwiązanie na tle konkurencji w postaci możliwości tworzenia „wysp I/O" oddalonych od sterownika centralnego.
- Obsługa złożonych logik programu – nie tylko przekaźniki bezpieczeństwa, ale również bardziej rozbudowane logiki programu są możliwe do sterowania poprzez dołożenie dodatkowej jednostki centralnej SAFETY PLC SC-1000 do sterownika nadrzędnego.

Moduły Safety SC-1000 oraz Safety I/O. Źródło: ASTOR



System z rozproszonymi modułami I/O. Źródło: ASTOR

Astraada One wykorzystuje otwarty standard CODESYS

Oprogramowanie CODESYS jest najbardziej otwartym środowiskiem programistycznym w świecie automatyki. Jest w pełni darmowe i przystosowane do adaptacji, dlatego też wielu największych producentów sterowników PLC decyduje się na wykorzystanie CODESYS jako głównego środowiska programistycznego. Dzięki otwartej strukturze bardzo szybko się rozwija. Potwierdza to duży zasób bibliotek, dzięki którym programowanie nawet zaawansowanych funkcjonalności często sprowadzone jest do kilku bloków i linijek kodu.

Oprogramowanie CODESYS daje możliwość tworzenia programów w oparciu o wszystkie języki określone w normach sterowników PLC. Dodatkowo wzbogaca je o język C, pozwalając na tworzenie jeszcze bardziej zaawansowanych programów. Wszystko to zawarte jest w intuicyjnym i czytelnym oknie, w którym nawet nowy użytkownik szybko się odnajdzie. •

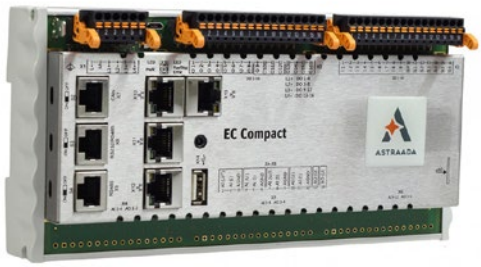
Czy opłaca się inwestować w sterowniki PLC z dwoma rdzeniami?

Porównanie sterowników z jednym i dwoma rdzeniami

Procesor jest sercem i mózgiem każdego sterownika PLC. Dla nas, użytkowników, najbardziej istotnym jego parametrem jest szybkość przetwarzania informacji. W skomplikowanych układach sterowania pożądane jest, aby procesor działał jak najszybciej. Procesory jednordzeniowe wykonują jedną operację w danym momencie. Niestety pomimo taktowania rzędu milionów razy na sekundę czasami nie jest to wystarczające. Rozwiązaniem są procesory wyposażone w więcej rdzeni obliczeniowych.

AUTOR: **Mateusz Pytel**
Menedżer produktu Astraada One
mateusz.pytel@astor.com.pl

» Poniżej przedstawiamy testy porównawcze sterownika Astrada One Compact ECC2200 i ECC2201 DUO. Ten drugi wyposażony jest w procesor Dual Core, który dzięki dwóm niezależnym rdzeniom może wykonywać dwie różne operacje w tym samym czasie, poprawiając tym samym wydajność. Sprawdzimy, jak to wygląda w praktyce.



W tabeli 1 zebrane są najważniejsze parametry obu tych sterowników.

MODEL	ECC2200	ECC2201 DUO
CPU	Freescale i.MX6 CPU 800MHz	Dual core: 800MHz ARM CPU Cortex-A9
Pamięć Flash	256 MB/ 100MB na aplikacje	1 GB
Pamięć RAM	256MB/ 128 MB na aplikacje	1 GB
Pamięć z podtrzymaniem	100 kB	100 kB
Interfejs Ethernet	1× 10/100 lub 3× 10/100	1× 10/100
Interfejs EtherCAT	1× RJ45	1× RJ45
Interfejs USB	1× USB 2.0	1× USB 2.0
Interfejs CAN Bus/open	1× CAN/RJ45	1× CAN/RJ45
Interfejs COM	1× RS232/RS485, 1× RS485	1× RS232/RS485, 1× RS485
Slot kart micro SD	Do 32 GB	Do 32 GB
Wejścia cyfrowe	16	16
Szybkie liczniki	Możliwość programowalnej aktywacji 2× HSC 500kHz	Możliwość programowalnej aktywacji 2× HSC 500kHz
Wyjścia cyfrowe	4×4 (0,5A)	4×4 (0,5A)
Wejścia analogowe	-	6× (+/-10V, +/-20mA PT100/ PT1000) 6× (+/-10V, +/-20mA)
Wyjścia analogowe	-	6× napięciowe (0-10V)

Tabela 1. Najważniejsze parametry obu sterowników

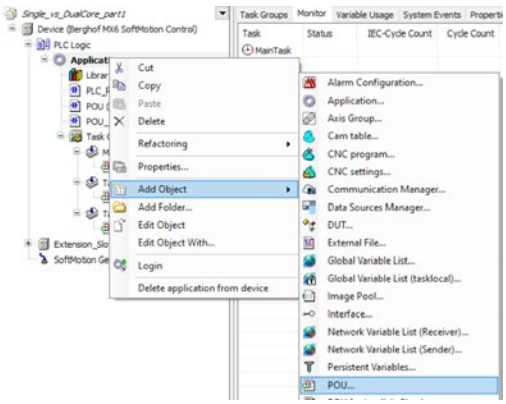
Przebieg testów

Przeprowadzono dwa testy, do których wykorzystano dwa różne kody: jeden cyklicznie ustawiał zmienne, a w drugim zaimplementowano dwa regulatory PID. Każdy z tych kodów zdublowano do nowego programu (POU), który przydzielono do innego tasku (zadania). **Następnie sterowniki wykonywały te programy – najpierw przydzielone w Task Configuration do jednego, a następnie do dwóch różnych rdzeni.** W każdym teście monitorowane były czasy cyklów, które są ściśle powiązane z wydajnością programu.

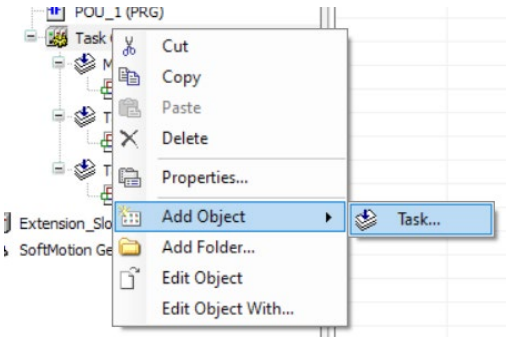
Scan time to czas cyklu potrzebnego na odczytanie danych wejściowych, przetworzenie i wykonanie obliczeń, obsługę interfejsów komunikacyjnych oraz ustawienie wyjść i autodiagnostykę. Im szybciej sterownik wykona te czynności, tym szybciej program może analizować i przetwarzać dane. Czas cyklu zależy między innymi od systemu operacyjnego oraz parametrów procesora

Jak podzielić taski na dwa rdzenie?

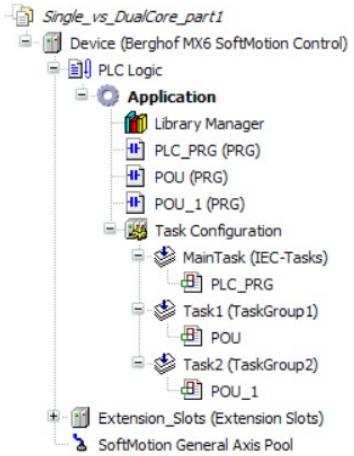
Pierwszym krokiem jest dodanie dwóch dodatkowych programów POU. Klikamy prawym przyciskiem myszy na zakładkę **Application** i wybieramy **Add Object → POU...**



Następnie dodajemy dwa nowe taski, klikając prawym przyciskiem myszy na pozycję **Task Configuration** i wybierając **Add Object → Task...**

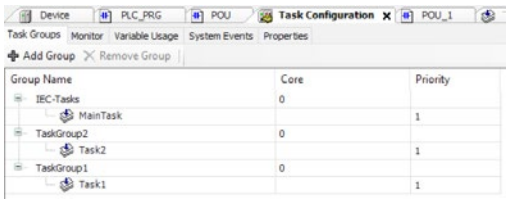


Następnie przeciągamy POU do poszczególnych tasków, aby końcowy rezultat był następujący:



PLC-PRG jest to program główny. Zostawiamy go pustego, ponieważ w nim oraz w Main Task wykonywane będą operacje systemowe, które zaciemnią nam wyniki testów. Chcemy oddzielić wykonywane programy od operacji wykonywanych w tle. W dwóch kolejnych POU umieszczamy docelowe programy testowe. W praktyce nie musimy robić takich podziałów i możemy zrealizować go tylko w dwóch POU i Task Group.

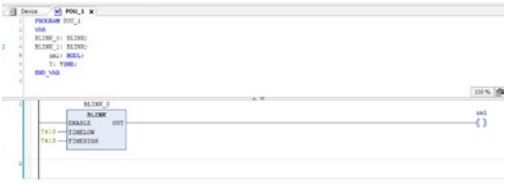
Przydzielamy taski do grup. Klikamy dwukrotnie w **Task Configuration** i dodajemy nową grupę przyciskiem **Add Group**. Możemy zmienić jej nazwę klikając na niej dwukrotnie. Następnie przeciągamy taski do odpowiednich grup. W kolumnie Core wybieramy numer rdzenia, na którym ma być wykonywany dany task.



Na końcu łączymy się ze sterownikiem, wgrywamy program (pamiętajmy o napisaniu i zdublowaniu kodu w naszych POU), przechodzimy w tryb RUN. W **Task Configuration** przechodzimy do zakładki **Monitor**.

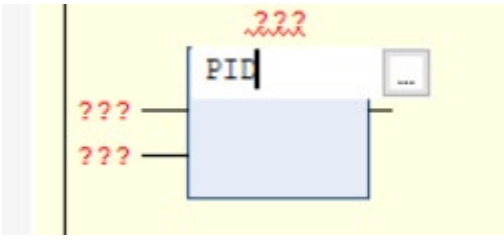
Program cyklicznie ustawiający zmienne

Wykonujemy prosty program cyklicznie zmieniający zmienną typu BOOL. W pełnym okresie cyklu przez jedną sekundę zmienna ma wartość 1, a przez jedną – wartość 0.

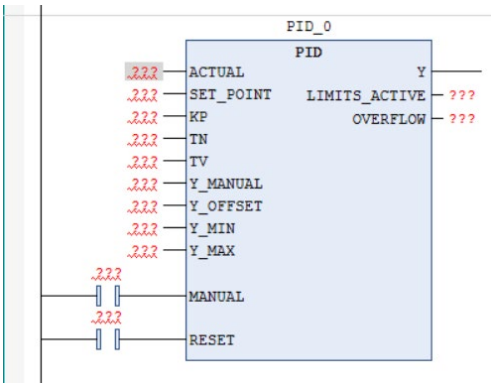


Program wykorzystujący regulatory PID

W tym programie dodajemy dwa moduły PID. Wykorzystujemy do tego blok **BOX** znajdujący się w zakładce **General**, w którym wpisujemy **PID** i wciskamy **Enter**. Pod każdym blokiem dodajemy blok sumy, który będzie dodawał nam wartość regulacji do wartości aktualnej.

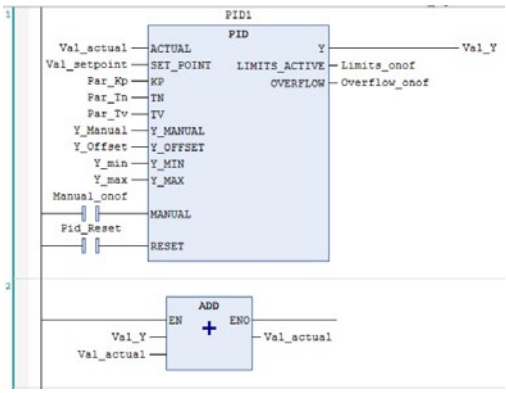


Otrzymujemy „goły” blok PID, do którego musimy teraz stworzyć zmienne. Nie wszystkie będą używane, natomiast wymagane jest ich zdefiniowanie. Przypisujemy im wartości startowe, które ustawią się wraz z włączeniem programu. Należy pamiętać, aby przed każdym testem wyzerować zmienne, które zawierają dane z poprzednich cykli testowych.



```
POU ✕ | POU_1 | Task Configuration
1  PROGRAM POU
2  VAR
3  // ---------WSPÓLNE---------- //
4      Manual_onof: BOOL := 0;
5      Pid_Reset: BOOL := 0;
6      Limits_onof: BOOL := 0;
7      Overflow_onof: BOOL := 0;
8      PID1: PID;
9      PID2: PID;
10 // ----------PID1------------ //
11     Val_Y: REAL;
12     Val_actual: REAL := 0;
13     Val_setpoint: REAL := 50;
14     Par_Kp: REAL := 0.05;
15     Par_Tn: REAL := 0.02;
16     Par_Tv: REAL := 0.00;
17     Y_Manual: REAL;
18     Y_Offset: REAL;
19     Y_min: REAL := -20;
20     Y_max: REAL := 20;
21 // ----------PID2------------ //
22     Val_Y2: REAL;
23     Val_actual2: REAL := 0;
24     Val_setpoint2: REAL := 70;
25     Par_Kp2: REAL := 0.07;
26     Par_Tn2: REAL := 0.03;
27     Par_Tv2: REAL := 0.0001;
28     Y_Manual2: REAL;
29     Y_Offset2: REAL;
30     Y_min2: REAL := -30;
31     Y_max2: REAL := 30;
32 END_VAR
33
```

Końcowy rezultat wygląda następująco:



Warto zaznaczyć, że dla tego programu zmieniono czas interwału tasków na 1000 ms, czyli 1 s. Dzięki temu regulatory PID trochę wolniej regulują sygnał.

Wyniki testów

Analizując wyniki będziemy patrzeć na **Average Cycle Time** mierzony w µs, który jest podawany przez sterownik podczas podglądu programu.

Program cyklicznie ustawiający zmienne

Poniżej przedstawiono porównanie danych pozyskanych po około 1000 cyklach programu. Jak widać, w sterowniku Dual Core zasoby przeznaczone na programy rozłożone są po równo, natomiast w sterowniku z jednym rdzeniem widać już lekkie dysproporcje, co jest spowodowane priorytetyzacją jednego z podprogramów. Przy bardziej skomplikowanych i dłuższych programach może to wpływać na wydajność całego systemu.

Task	Status	IEC-Cycle Count	Cycle Count	Configure...	Last Cycle Time (µs)	Average Cycle Time (µs)	Max. Cycle Time (µs)	Min. Cycle Time (µs)	Jitter (µs)	Min. Jitter (µs)	Max. Jitter (µs)	Core
MainTask	Valid	1025	1025	25 ms	115	91	116	82	1	-24	26	0
Task1	Valid	1025	1025	25 ms	11	10	21	9	-7	-20	17	0
Task2	Valid	1025	1025	25 ms	15	15	38	12	-3	-17	22	0

Wyniki dla sterownika jednordzeniowego EC2200. Źródło: ASTOR

Task	Status	IEC-Cycle Count	Cycle Count	Configure...	Last Cycle Time (µs)	Average Cycle Time (µs)	Max. Cycle Time (µs)	Min. Cycle Time (µs)	Jitter (µs)	Min. Jitter (µs)	Max. Jitter (µs)	Core
MainTask	Valid	1032	1032	25 ms	113	93	127	79	-2	-39	31	0
Task1	Valid	1032	1032	25 ms	11	12	25	10	5	-30	30	0
Task2	Valid	1032	1032	25 ms	14	12	18	9	-3	-11	13	1

Wyniki dla sterownika dwurdzeniowego EC2201. Źródło: ASTOR

Program cyklicznie ustawiający zmienne

Task	Status	IEC-Cycle Count	Cycle Count	Configure...	Last Cycle Time (µs)	Average Cycle Time (µs)	Max. Cycle Time (µs)	Min. Cycle Time (µs)	Jitter (µs)	Min. Jitter (µs)	Max. Jitter (µs)	Core
MainTask	Valid	120	120	1000 ms	98	103	145	83	43	-45	55	0
Task1	Valid	120	120	1000 ms	21	22	26	20	8	-14	12	0
Task2	Valid	120	120	1000 ms	28	29	51	27	9	-11	17	0

Wyniki dla sterownika jednordzeniowego EC200 bez rozdzielenia na rdzenie. Źródło: ASTOR

Task	Status	IEC-Cycle Count	Cycle Count	Configure...	Last Cycle Time (µs)	Average Cycle Time (µs)	Max. Cycle Time (µs)	Min. Cycle Time (µs)	Jitter (µs)	Min. Jitter (µs)	Max. Jitter (µs)	Core
MainTask	Valid	120	120	1000 ms	104	98	118	84	11	-72	51	0
Task2	Valid	120	120	1000 ms	23	32	190	21	-4	-173	131	0
Task3	Valid	120	120	1000 ms	30	41	254	27	11	-183	43	0

Wyniki dla sterownika dwurdzeniowego EC201 bez rozdzielenia na rdzenie. Źródło: ASTOR

Task	Status	IEC-Cycle Count	Cycle Count	Configure...	Last Cycle Time (µs)	Average Cycle Time (µs)	Max. Cycle Time (µs)	Min. Cycle Time (µs)	Jitter (µs)	Min. Jitter (µs)	Max. Jitter (µs)	Core
MainTask	Valid	120	120	1000 ms	243	115	315	84	-3	-147	37	0
Task2	Valid	120	120	1000 ms	44	29	189	22	-1	-153	42	0
Task3	Valid	120	120	1000 ms	25	25	30	22	-3	-8	7	1

Wyniki dla sterownika dwurdzeniowego EC201 z rozdzieleniem na rdzenie. Źródło: ASTOR

Task	Status	IEC-Cycle Count	Cycle Count	Configure...	Last Cycle Time (µs)	Average Cycle Time (µs)	Max. Cycle Time (µs)	Min. Cycle Time (µs)	Jitter (µs)	Min. Jitter (µs)	Max. Jitter (µs)	Core
MainTask	Valid	120	120	1000 ms	271	116	303	86	-6	-168	41	0
Task2	Valid	120	120	1000 ms	19	18	24	16	-9	-132	142	1
Task3	Valid	120	120	1000 ms	35	34	41	24	-3	-16	11	1

Wyniki dla sterownika dwurdzeniowego EC201 z dwoma programami na osobnym rdzeniu. Źródło: ASTOR

Jak można zauważyć, tam gdzie programy są przydzielone do tego samego rdzenia, występują dysproporcje w czasie cyklu poszczególnych tasków, a w przypadku obydwu programów działających w odosobnieniu od Main Taska ta różnica jest największa, bo aż 16 mikrosekund. Oznacza to, że jeden program działa szybciej od drugiego, co przy większej skali projektu może negatywnie wpływać na efektywność. Kiedy programy były na dwóch osobnych rdzeniach, różnica ta była najmniejsza.

Wnioski

Na podstawie przeprowadzonych testów możemy odpowiedzieć sobie na pytanie zawarte w tytule artykułu i wywnioskować, że sterowniki z dwoma rdzeniami mają wyraźną przewagę. Dzięki możliwości przypisania różnych zadań do rożnych rdzeni możemy zwiększyć wydajność i szybkość operacji, co jest kluczowe w układach sterowania wymagających szybkości i wykonywania dużej ilości obliczeń. Możemy także rozdzielić zadania, aby zwiększyć ogólną szybkość sterownika lub podzielić na zadania mniej i bardziej priorytetowe. •

→ Jak korzystać z połączenia FTP i VNC w panelach Astraada HMI?

FTP (File Transfer Protocol) to protokół sieciowy, który umożliwia transfer plików pomiędzy dwoma urządzeniami, pracującymi w konfiguracji klient-serwer. FTP wykorzystywane jest w przypadku, gdy za pomocą sieci Ethernet chcemy mieć zdalny dostęp do plików takich, jak np. receptury czy logi operacyjne, które znajdują się w panelach HMI. FTP pozwala na pobieranie plików i przekazywanie ich na inne urządzenie, gdzie możemy je dowolnie analizować i modyfikować.

» **VNC (Virtual Network Computing)** to system zdalnego dostępu, który ma możliwość przekazywania obrazu. Dzięki niemu uzyskujemy zdalny dostęp do ekranu danego urządzenia. Tym samym mamy możliwość monitorowania oraz kontrolowania aplikacji wizualizacyjnej poprzez sieć Ethernet.

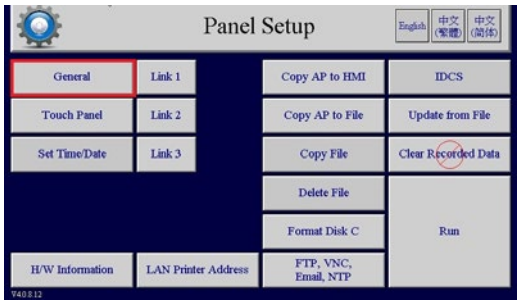
VNC pozwala na zdalną obsługę panelu operatorskiego Astraada HMI za pomocą konsoli VNC zainstalowanej na komputerze. Z tej opcji korzystają służby utrzymania ruchu do jednoczesnej kontroli wszystkich paneli w systemie, analizy sygnałów diagnostycznych czy dokonywania zmian w menu. Ważne jest, że panele Astraada HMI mogą być jedynie serwerem VNC, nie klientem.

Warto też nadmienić, czym jest NTP, o którym wspomnimy w dalszej części artykułu. **NTP** (Network Time Protocol) to protokół, który służy do synchronizacji czasu z zewnętrznym nadrzędnym urządzeniem.

Konfiguracja FTP, VNC i NTP

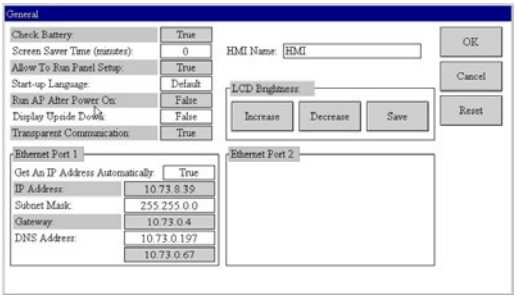
Na samym początku warto zaznaczyć, że aby FTP i VNC poprawnie funkcjonowały, panel musi pracować w wersji firmware minimum 2.0. Jeżeli do programowania panela użyjemy aplikacji Astraada HMI CFG w wersji co najmniej 2.0, panel zostanie automatycznie zaktualizowany.

Pracę z FTP i VNC należy rozpocząć od uruchomienia panelu i wprowadzenia zmian w menu **Panel Setup**. Należy wejść w zakładkę **General**, jak pokazano poniżej:



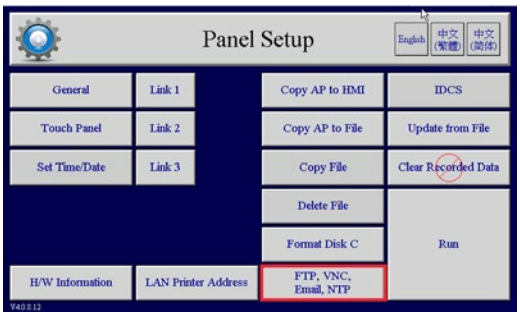
W sekcji **Ethernet Port 1** ustawiamy pole **Get An IP Address Automatically** na **True**. Jeśli w sieci, do której wpinamy panel, działa serwer DHCP, to adres IP ustawi się automatycznie.

W innym wypadku sami wpisujemy odpowiedni adres IP i podajemy prawidłową maskę podsieci. Kolejno uzupełniamy adres bramy sieciowej, co pozwoli panelowi HMI na komunikację z innymi urządzeniami. Następnie wprowadzamy adresy serwerów DNS. Adres IP, Subnet Mask, Gateway oraz DNS Address muszą być odpowiednio uzupełnione. W przypadku gdy potrzebujesz dokładnych instrukcji bądź wsparcia technicznego w temacie konfiguracji sieciowej – skontaktuj się z działem IT, który doradzi jak zrobić to poprawnie na Twoim urządzeniu.



Przyciskiem OK zatwierdzamy wprowadzone zmiany.

Następnie wybieramy opcję **FTP, VNC, Email, NTP**:

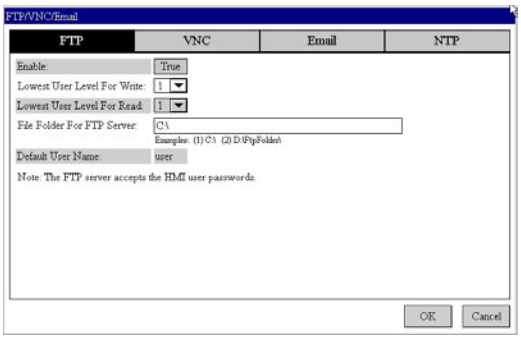


AUTOR: **Karolina Niziołek**

Asystentka ds. obsługi sklepu internetowego

karolina.niziolek@astor.com.pl

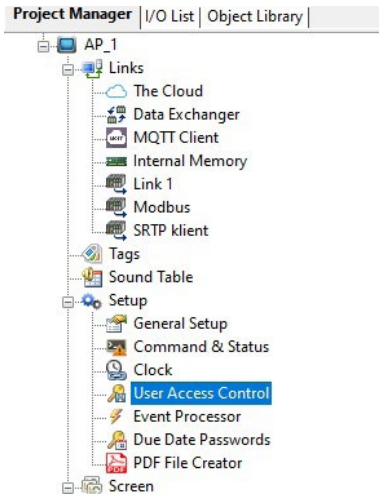
W zakładce **FTP** konfigurujemy poszczególne pola:



Zmieniamy wartość **Enable** na **True**.

Kolejno ustalamy najmniejsze poziomy dostępu, jakie musi posiadać zalogowany użytkownik, aby wgrywać (**Lowest User Level For Write**) oraz pobierać pliki (**Lowest User Level For Read**).

Poziom użytkownika jest powiązany z hasłami, jakie będzie musiał on wprowadzić w trakcie logowania się do FTP. Hasła te określone są w aplikacji Astraada HMI CFG w zakładce **User Access Control**:



Jeśli chcesz wiedzieć więcej na temat haseł operatorskich, zapraszamy do 12 odcinka naszego kursu programowania paneli HMI: https://www.astor.com.pl/poradnikautomatyka/jak-ograniczyc-dostep-do-aplikacji-hasla-operatorskie-kurs-hmi-12/

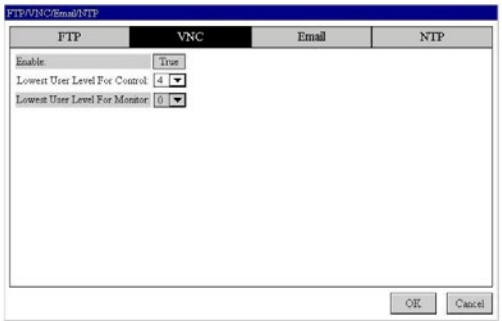
Kolejne pole w omawianej przez nas zakładce FTP to **File Folder For FTP Server**, czyli lokalizacja folderu plików dla serwera FTP.

Organizacja dysków w panelu Astraada jest następująca:

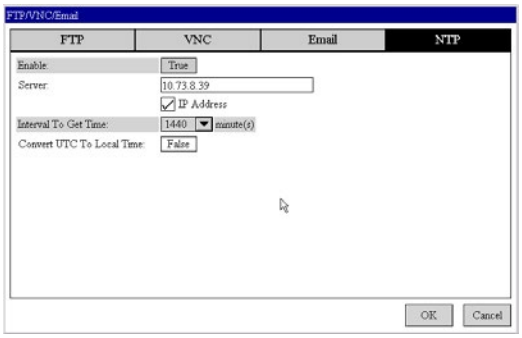
- Dysk C:\ – wewnętrzna pamięć flash.
- Dysk D:\ – karta Micro SD (jeśli obecna).
- Dysk E:\ – masowa pamięć w porcie USB (jeśli obecna).

Ostatnie pole to **Default User Name**, czyli nazwa użytkownika, którą musimy podać przy logowaniu do FTP.

W przypadku konfiguracji zakładki **VNC** należy najpierw włączyć funkcjonalność VNC w panelu poprzez zmianę wartości **Enable** na **True**. Następnie, analogicznie jak wcześniej, ustawiamy najniższe poziomy dostępu użytkowników, jakie są potrzebne do modyfikacji parametrów (**Lowest User Level For Control**) i monitorowania ekranów (**Lowest User Level For Monitor**).



Kolejno otwieramy zakładkę **NTP**. Najpierw zmieniamy wartość **Enable** na **True**. Pole **Server** możemy uzupełnić o nazwę odnoszącą się do serwera bądź zaznaczyć checkbox **IP Address** i wpisać odpowiedni adres IP.



Przyciskiem OK zatwierdzamy wprowadzone zmiany.

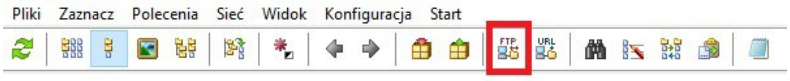
Istnieje także zakładka **Email**, w której po wpisaniu odpowiednich danych możemy otrzymywać wiadomości na skrzynkę pocztową wraz z załącznikami i plikami z panelu.

Połączenie FTP w panelach Astraada HMI

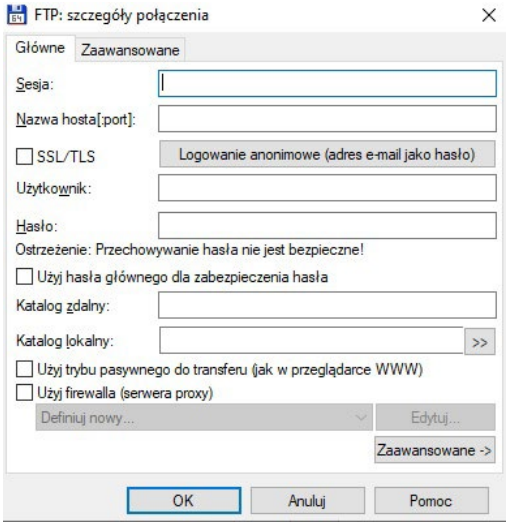
Żeby dokonać połączenia, trzeba pamiętać o odpowiedniej konfiguracji zabezpieczenia systemu operacyjnego, tak aby uniknąć blokowania połączenia.

Najpierw należy zalogować się do FTP. Możemy skorzystać z przeglądarki internetowej, eksploratora plików bądź narzędzia takiego jak Total Commander. W pasku wyszukiwania przeglądarki lub w ścieżce eksploratora plików należy wpisać ftp://aaa.bbb.ccc.ddd, gdzie aaa.bbb.ccc.ddd to adres IP panelu, który możemy sprawdzić w **Panel Setup** w zakładce **General**.

W przypadku gdy korzystamy z Total Commander, należy kliknąć ikonę zaznaczoną na rysunku, następnie wybrać opcję **Nowe Połączenie**.



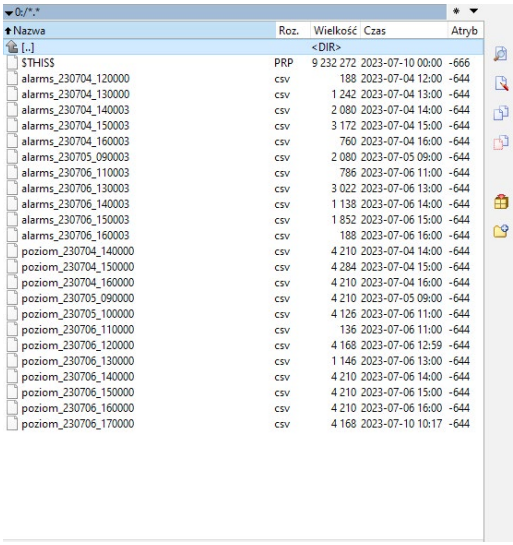
Konfigurujemy okno **FTP: szczegóły połączenia**.

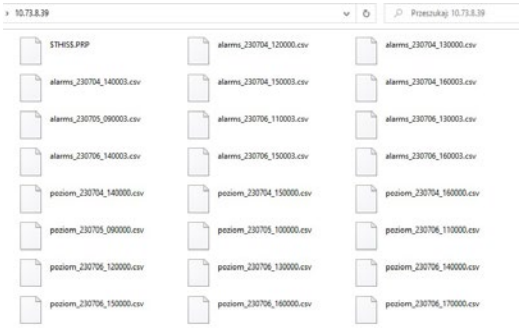


W polu **Sesja** wpisujemy dowolną nazwę. **Nazwa hosta[:port]** to adres IP naszego panelu HMI. Pola **Użytkownik** i **Hasło** uzupełniamy o dane wprowadzone w aplikacji w zakładce **User Access Control** odpowiednio dla ustawionego poziomu dostępu dla połączenia FTP. Zaznaczamy również opcję **Użyj trybu pasywnego do transferu (jak w przeglądarce WWW)**.

Po naciśnięciu przycisku OK i zalogowaniu powinniśmy otrzymać dostęp do plików panelu.

Poniżej dla przykładu przedstawiono jak wygląda to dla połączenia wykonanego w Total Commander oraz eksploratorze plików.

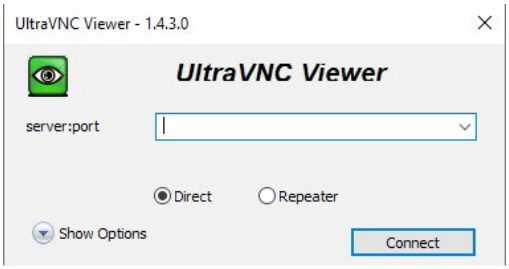




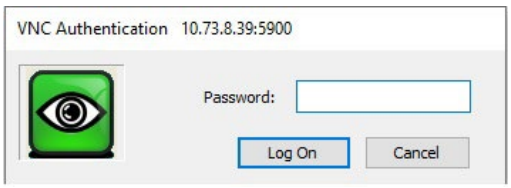
Połączenie VNC w panelach Astraada HMI

W celu zalogowania się do VNC potrzebujemy dostępu do oprogramowania na komputerze bądź smartfonie. Korzystamy z dowolnej aplikacji przeznaczonej dla tego typu połączeń. W poniższym przykładzie wykorzystamy UltraVNC Viewer.

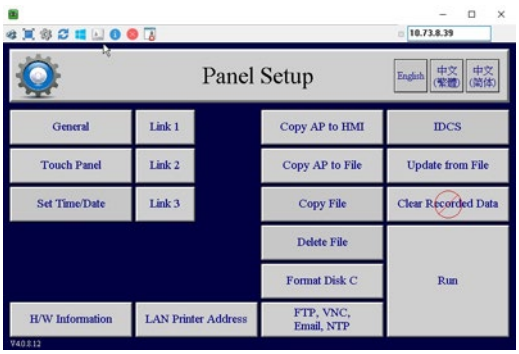
Po włączeniu konsoli zostaniemy poproszeni o wpisanie adresu IP panelu w polu **server:port**.

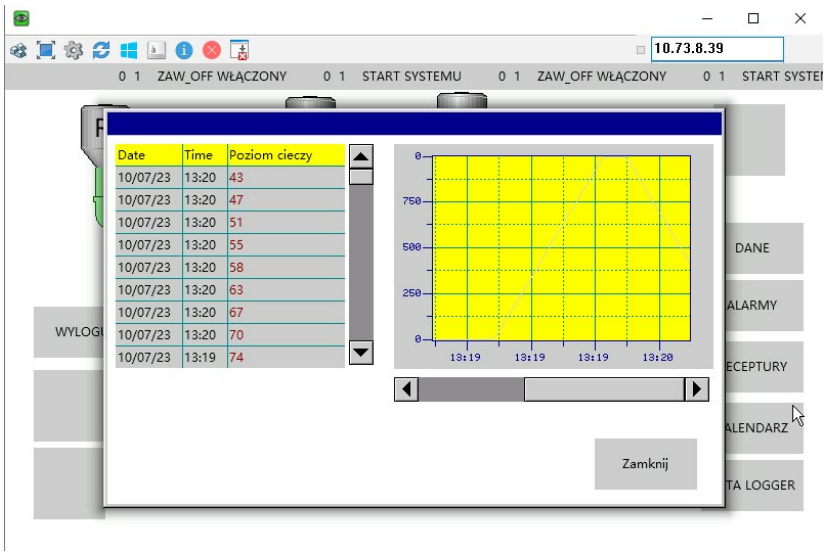


Po naciśnięciu przycisku **Connect** pokaże nam się kolejne okno, w którym należy wpisać hasło dostępu, które ustawiliśmy w aplikacji Astraada HMI CFG w zakładce **User Access Control** dla minimalnego poziomu użytkownika zdefiniowanego w ustawieniach VNC.



Po wciśnięciu klawisza **Log On** powinniśmy uzyskać zdalny dostęp do panelu HMI.





Warto zaznaczyć, że zalogowanie się przez VNC do panelu nie powoduje zmiany aktualnie zalogowanego użytkownika.

Podsumowanie

FTP pozwala na dostęp do plików oraz ich transferowanie. Zdalnie możemy łączyć się z panelem HMI, eksportować dane i w łatwy sposób je analizować.

VNC umożliwia połączenie z panelem HMI, monitorowanie i kontrolowanie aplikacji za pomocą sieci Ethernet.

Rozwiązania te znacznie przyspieszają i ułatwiają pracę ze względu na fakt, że w sieci lokalnej jesteśmy w stanie połączyć się z panelem, eksportować dostępne pliki i sterować aplikacją.

Warto zaznaczyć, że VNC służy do zdalnego łączenia z panelem HMI wyłącznie do celów serwisowych. Nie jest zalecane długotrwałe połączenie ze względu na fakt, że stabilność działania jest zależna od jakości połączenia konsoli VNC z panelem. W wyniku wielogodzinnego działania VNC, panel może ulec zawieszeniu. •

CYFROWY BLIŹNIAK 4.0

Technologiczna odpowiedź na dynamicznie zmieniający się świat przemysłu

W erze Czwartej Rewolucji Przemysłowej, technologia cyfrowego bliźniaka staje się kluczem do zrozumienia przyszłości przemysłu. Jeśli czujesz, że potrzebujesz wiedzy, by nadążyć za zmianami w **dobie cyfrowej transformacji**, ASTOR, lider w dziedzinie Przemysłu 4.0, ma dla Ciebie białą księgę [whitepaper] o budowie cyfrowych baz danych w przemyśle.

„Cyfrowy bliźniak 4.0" rzuca światło na różne aspekty tej innowacji - od jej podstaw po zaawansowane zastosowania. I podkreśla, że **przyszłość przemysłu jest cyfrowa**, a cyfrowy bliźniak jest jednym z jej filarów.

Jak zatem skopiować fabrykę? Jakie korzyści biznesowe niesie za sobą cyfrowy bliźniak? Jak go praktycznie zastosować? Odpowiedź jest w zasięgu ręki!

ASTOR
gdzie technologia spotyka człowieka

www.astor.com.pl/whitepaper-cyfrowy-blizniak-4-0

Windows IoT czy Professional? Jaki system operacyjny wybrać dla komputera przemysłowego?

Komputer przemysłowy (IPC) ma wiele cech, które odróżniają go od zwykłego domowego peceta. Wciąż jednak jest to komputer klasy PC, a więc by uruchomić na nim jakiekolwiek oprogramowanie, najpierw musimy zainstalować system operacyjny.

» Przeglądając oferty komputerów przemysłowych z systemem Windows możemy zauważyć, że dostarczane są one najczęściej z jedną z dwóch wersji tego systemu: Windows 10/11 Pro lub Windows 10/11 IoT. Ta pierwsza nazwa brzmi znajomo dla każdego użytkownika komputera PC, ale czym jest Windows IoT?

Rozwiązanie dla systemów wbudowanych

Wskazówką może być oczywiście sama nazwa. Skrót IoT oznacza „Internet of Things" (Internet Rzeczy). Windows IoT to rodzina systemów operacyjnych, zoptymalizowanych i przeznaczonych do wykorzystania w aplikacjach specjalnych, w tym w automatyce przemysłowej, systemach wbudowanych (embedded) i urządzeniach Internetu Rzeczy. W przemyśle typowym zastosowaniem są tu oczywiście stacje operatorskie (SCADA), wykorzystujące komputery przemysłowe z wbudowanym ekranem.

Optymalizacja dotknęła dwóch najważniejszych obszarów. Po pierwsze jej celem było zwiększenie wydajności, po drugie – chodziło o maksymalizację niezawodności i bezpieczeństwa systemu.

Komputer pracujący w zastosowaniach przemysłowych powinien być oczywiście odpowiednio wydajny, ale wydajność ta musi być stabilna. W uproszczeniu można powiedzieć, że komputer musi działać cały czas tak samo dobrze. Dlatego w Windows IoT zoptymalizowano wydajność, usuwając niektóre usługi bądź aplikacje (próżno tu szukać np. Windows Store albo obsługi gier i konsol). Najistotniejsze różnice pomiędzy wersjami Pro i IoT kryją się jednak w obszarze bezpieczeństwa.

Zaawansowane zabezpieczenia w Windows IoT

System Windows IoT oddaje w ręce administratorów cały szereg narzędzi i opcji, zwiększających poziom bezpieczeństwa, wspólnie określanych jako **Advanced Lockdown Features** (zaawansowane funkcje zabezpieczeń dostępu). Pozwalają one skutecznie chronić urządzenie przed niedozwolonymi manipulacjami ze strony użytkowników, zarażeniem złośliwym oprogramowaniem, utratą danych lub nieuprawnionym dostępem – ze strony osób lub urządzeń.

Podstawowym elementem systemu zabezpieczeń jest **kontrola aplikacji** (Application Control), czyli rozwiązanie umożliwiające nadzór nad uruchamianiem aplikacji przez poszczególnych użytkowników. Windows IoT zawiera dwa rozwiązania w tym zakresie: **Windows Defender Application Control** (WDAC) oraz **AppLocker**. Oba pozwalają ściśle kontrolować, które aplikacje oraz sterowniki mogą być uruchamiane na urządzeniach z systemem Windows IoT, a także którzy użytkownicy mogą te aplikacje uruchamiać.

Drugą ciekawą funkcją charakterystyczną dla systemu Windows IoT jest **Jednolity Filtr Zapisu** (Unified Write Filter, UWF). Pomaga ona chronić system i zawartość dysku, przekierowując wszystkie zapisy na nim do specjalnego dysku wirtualnego, który może być czyszczony podczas ponownego uruchamiania systemu. Dzięki temu żadne zmiany

AUTOR: **Mateusz Fas**
Młodszy specjalista ds. sprzedaży internetowej
mateusz.fas@astor.com.pl

Rys. 1. Komputer przemysłowy Astraada PC typu Box. Źródło: ASTOR

Rys. 2 Komputer przemysłowy Astraada PC z aplikacją wizualizacyjną. Źródło: ASTOR

wprowadzone podczas użytkowania systemu nie będą zapamiętane.

UWF może ponadto współdziałać z funkcją **HORM** (Hibernate Once/Resume Many), dzięki czemu urządzanie jest uruchamiane zawsze w tym samym, prekonfigurowanym stanie. W takim przypadku komputer może być bez szkody szybko wyłączony (np. wskutek odcięcia zasilania), a gdy zostanie ponownie włączony, otrzymujemy środowisko bez zmian, gotowe do pracy.

Inną przydatną funkcją są **filtry wejścia** (Input Filters). Należą do nich **filtr klawiatury** (Keyboard Filter) i **filtr USB** (USB Filter). Ten pierwszy pozwala zdefiniować, które klawisze i skróty klawiszowe są aktywne w systemie, a które zostaną zablokowane. Przykładowo możemy zablokować skróty Ctrl + Alt + Del oraz Alt + F4, aby zabezpieczyć dostęp do funkcji przez nie wywoływanych. Z kolei filtr USB pozwala określić, które urządzenia podłączane przez porty USB będą dozwolone, a które zablokowane. Możemy np. zablokować dostęp do pamięci typu Pendrive, blokując w ten sposób możliwość przenoszenia danych lub aplikacji.

Kontrola nad aktualizacjami

Systemy Microsoft Windows wyposażone są w mechanizm automatycznej instalacji aktualizacji – Windows Update. Zapewnia on samoczynną instalację poprawek bezpieczeństwa oraz aktualizacji funkcjonalnych. Administratorzy sieci firmowych wiedzą jednak doskonale, że automatyczna instalacja aktualizacji nie zawsze jest najlepszym rozwiązaniem, szczególnie na komputerach o krytycznym znaczeniu, co jest częste w zastosowaniach przemysłowych.

Po pierwsze, zdarza się, że aktualizacje mogą powodować problemy z działaniem niektórych aplikacji. Po drugie – sam proces aktualizacji poważnie zakłóca pracę komputera, powodując jego większe obciążenie, a także wymuszając restart systemu. Osobną sprawą jest konieczność zapewnienia stałego dostępu do Internetu. Po dłuższym odłączeniu komputera od sieci usługa Windows Update często zgłasza konieczność zainstalowania dziesiątek aktualizacji, co mocno dezorganizuje działanie systemu.

Z tych właśnie powodów w systemie Windows IoT wprowadzono możliwość **zarządzania aktualizacjami Windows Update przez administratora**. Obejmuje to również opcję całkowitego wstrzymania ich instalacji. Dzięki temu administrator może w pełni kontrolować proces aktualizacji, realizując go w dogodnych momentach (np. w zaplanowanych przerwach serwisowych), a także instalując tylko przetestowane aktualizacje, które nie będą stanowiły zagrożenia dla ciągłości pracy systemu i aplikacji.

Core czy Enterprise?

Uważny Czytelnik z pewnością spostrzegł, iż na początku wspomnieliśmy o *rodzinie systemów*. Pod nazwą Windows IoT kryje się bowiem kilka różnych wersji tego systemu, z których najbardziej interesują nas **Windows IoT Core** oraz **Windows IoT Enterprise**. Warto w tym miejscu krótko wspomnieć, czym one się różnią.

Rys. 3. Komputer przemysłowy Astraada PC z aplikacją wizualizacyjną AVEVA Edge. Źródło: ASTOR

Wszystko, co wyżej pisaliśmy o funkcjonalności Windows IoT, zasadniczo odnosi się do wersji Enterprise. Jest to podstawowa wersja tego systemu, która bazuje na pełnej wersji Windows 10/11 Enterprise. Producent informuje, że jest to *binarny odpowiednik* (binary equivalent) systemu Windows 10/11 Enterprise, rozszerzony o zaawansowane mechanizmy bezpieczeństwa (opisane powyżej). Fakt, iż mamy do czynienia z binarnym odpowiednikiem, oznacza niemal pełną zgodność obu systemów – możemy używać tych samych programów i narzędzi, co w standardowych Windowsach.

Z kolei Windows IoT Core jest wersją ograniczoną, przeznaczoną do prostszych i mniejszych zastosowań. Krótko wspomnijmy o najważniejszych ograniczeniach. W wersji Core tylko jedna aplikacja może działać na pierwszym planie w danej chwili, a dodatkowo może to być tylko aplikacja UWP (Universal Windows Platform). Aplikacje Win32 mogą być uruchamiane wyłącznie w tle, bez interfejsu użytkownika (z dostępem np. przez Remote Access).

Windows Professional czy IoT?

Jak wspomnieliśmy wyżej, Windows 10/11 IoT Enterprise oferuje wszystkie funkcje i możliwości standardowego systemu Windows 10/11 Enterprise, uzupełnione dodatkowo o wiele dodatkowych, w szczególności związanych z bezpieczeństwem. Biorąc to pod uwagę można stwierdzić, że w zdecydowanej większości przypadków wersja IoT Enterprise będzie lepszym wyborem dla systemów wbudowanych.

Można tu krótko wymienić jeszcze kilka innych korzyści. Zasady licencjonowania Windows IoT są tak skonstruowane, a ceny licencji tak dobrane, że rozwiązanie to jest bardziej ekonomiczne, niż „zwykły" Windows. Ponadto systemy IoT objęte są znacznie dłuższym wsparciem serwisowym firmy Microsoft (nawet 10 lat). Dla niektórych użytkowników znaczenie może mieć i taka ciekawostka, jak możliwość samodzielnego „brandowania" systemu (można np. usunąć logo systemu operacyjnego Windows).

Kluczową sprawą jednak jest zgodność oprogramowania, którego zamierzamy używać, z wybraną przez nas wersją systemu. Dlatego przede wszystkim należy się kierować wskazówkami i wymaganiami formułowanymi przez producentów aplikacji, którzy jasno deklarują, jakie systemy operacyjne są przez nich wspierane, a jakie nie. Pamiętać trzeba, że producent nigdy nie gwarantuje poprawnej pracy aplikacji na niewspieranym sprzęcie lub systemie operacyjnym, a tym samym nie zapewnia on również w takim przypadku serwisu.

Przykładowo **oprogramowanie CODESYS Control RTE SL, które zapewnia funkcjonalność Soft PLC, jest w pełni zgodne z systemem Windows IoT Enterprise**. Dzięki temu możliwe jest uruchomienie sterowania typu Soft PLC na komputerze przemysłowym, pracującym pod kontrolą tego systemu.

Oprogramowanie AVEVA a Windows IoT

Jak wspomnieliśmy na wstępie, typowym „przemysłowym" zastosowaniem systemu Windows IoT, zainstalowanego na komputerze IPC, są stacje operatorskie SCADA. Warto więc na zakończenie podkreślić, że zarówno oprogramowanie wizualizacyjne **AVEVA Edge**, jak i oprogramowanie **AVEVA InTouch HMI 2023 są w pełni zgodne z systemem operacyjnym Windows 10/11 IoT Enterprise**. Producent zapewnia również zgodność z tym systemem innych aplikacji, w tym Application Server 2023, Historian Server 2023 oraz pozostałych komponentów Platformy Systemowej AVEVA 2023. •

Na co zwrócić uwagę przy doborze falownika do fotowoltaiki?

Gdyby porównać instalację fotowoltaiczną do ludzkiego ciała, falownik byłby sercem, mózgiem, płucami, wątrobą i nerkami. Krótko mówiąc: jest ważny.

AUTOR: **Piotr Knapik**
Opiekun produktów Astraada, ASTOR
piotr.knapik@astor.com.pl

» Falownik pełni bardzo wiele funkcji, od podstawowej – zamiany prądu stałego (produkowanego przez panele) na prąd przemienny, poprzez komunikację, a na monitorowaniu, diagnostyce błędów i rejestrowaniu danych kończąc. Można powiedzieć, że urządzenie to zarządza całym systemem fotowoltaicznym.

Wybór typu instalacji

Decydując się na przydomową elektrownię słoneczną musimy brać pod uwagę wiele czynników. Wśród nich są: orientacja dachu, zacienienie, szerokość geograficzna, zapotrzebowanie na energię elektryczną oraz napięcie w sieci. Każdy z tych parametrów ma bezpośredni wpływ na produkcję prądu przez instalację. Źle dobrane parametry mogą spowodować niższe uzyski, niż zakładaliśmy, co przełoży się na wydłużenie czasu zwrotu inwestycji.

Typy instalacji fotowoltaicznych

Wyróżniamy trzy typy systemów Instalacji fotowoltaicznych:

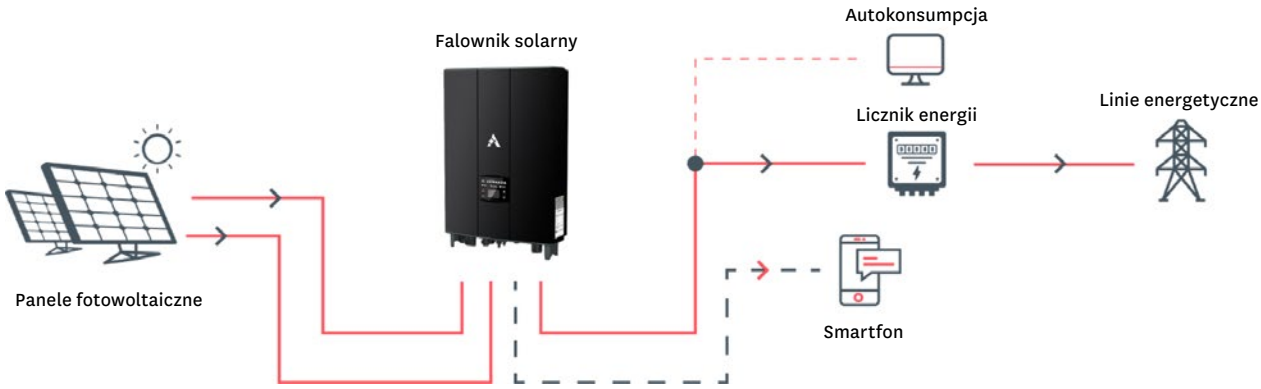
- **On-grid (sieciowe):** najczęściej występujący typ. W tym modelu wyprodukowany nadmiar energii elektrycznej oddawany jest do sieci energetycznej.
- **Hybrydowe (mieszane):** w tym modelu mamy połączenie sieciowej instalacji z magazynem energii. Instalacja w pierwszej kolejności ładuje akumulator, nadmiar wyprodukowanej energii oddaje do sieci. Rozwiązanie to daje dużą niezależność, jest też najdroższe.
- **Off-grid (niezależne):** instalacja nie jest przyłączona do sieci energetycznej, nastawiona jest tylko na ładowanie magazynu energii. Rozwiązanie stosowane tam, gdzie nie ma dostępu do publicznej sieci energetycznej.

Dopasowywanie modułów fotowoltaicznych do falowników

Dobierając panele fotowoltaiczne do falownika musimy zwrócić uwagę na technologię modułu fotowoltaicznego oraz na typ izolacji inwertera (beztransformatorowy / transformatorowy). Klasyczne panele zbudowane z ogniw monokrystalicznych lub polikrystalicznych, a także cienkowarstwowe ogniwa CIS/CIGS najczęściej mogą współpracować zarówno z falownikami beztransformatorowymi, jak i transformatorowymi.

Sytuacja komplikuje się przy panelach cienkowarstwowych CdTe oraz amorficznych. Ten typ paneli wymaga uziemienia ujemnego bieguna generatora PV. Umożliwia to jedynie falownik transformatorowy galwanicznie izolowany. W wypadku paneli typu *all back contact*, które mają skłonność do polaryzacji, również należy zastosować falownik transformatorowy, z uziemieniem bieguna dodatniego.

Tabela na stronie obok przestawia najczęstsze dopasowanie falowników do technologii modułów fotowoltaicznych.



Rys. 1. Schemat instalacji fotowoltaicznej z falownikiem Astraada SUN. Źródło: ASTOR

TECHNOLOGIA MODUŁÓW FOTOWOLTAICZNYCH	FALOWNIK BEZTRANSFORMATOROWY	FALOWNIK TRANSFORMATOROWY	FALOWNIK TRANSFORMATOROWY Z UZIEMIENIEM MINUSA	FALOWNIK TRANSFORMATOROWY Z UZIEMIENIEM PLUSA
Krzemowe krystaliczne mono/poli	×	×		
Cienkowarstwowe CdTe			×	
Cienkowarstwowe CIGS/CIS	×	×		
Cienkowarstwowe amorficzne			×	
Krzemowe ze skłonnością do polaryzacji (N-type)				×

Moc modułów PV a moc falownika

Producenci paneli fotowoltaicznych zalecają, aby moc paneli wahała się w przedziale 80-120% mocy falownika. Sprawność systemu jest najwyższa, gdy moc paneli zostanie przewymiarowana w stosunku do mocy falownika w granicach od 105 do 120%. Wynika to z panujących w Polsce warunków klimatycznych, z powodu których panele fotowoltaiczne prawie nigdy nie osiągają mocy nominalnej, wyznaczonej w warunkach STC. Dodatkowo zakurzenie modułów, rosnąca temperatura oraz przewody powodują spadek mocy.

Minimalne oraz maksymalne napięcia łańcuchów modułów fotowoltaicznych

Napięcie modułów jest uzależnione od temperatury, dlatego dobierając instalację PV konieczne jest wyznaczanie napięcia łańcucha modułu PV w granicznych dla niego temperaturach. Przyjmuje się, że górna granica temperatur modułów waha się w zakresie 65-70 stopni C. W przypadku minimalnej temperatury, można przyjąć zakres -16 do -24 stopni C.

Falowniki pracują w określonym zakresie napięcia wejściowego. Im szerszy zakres, tym większa elastyczność w liczbie modułów dobranych do danego MPPt. W przypadku falowników Astraada SUN zakres napięcia wejściowego wynosi 200-800 V.

Obliczanie minimalnej i maksymalnej liczby modułów PV w łańcuchu

Falowniki mają ściśle określony zakres napięcia wejściowego, w jakim mogą pracować. Dany szereg modułów musi dostarczyć napięcie robocze w zakresie pracy MPPt falownika z uwzględnieniem zarówno niskiej, jak i wysokiej temperatury. Większość paneli fotowoltaicznych posiada napięcie wyjściowe około 30 V.

Rys. 2. Falownik fotowoltaiczny Astraada SUN. Źródło: ASTOR

Napięcie wejściowe falowników jest różne. Posłużmy się przykładem falowników Astraada Sun, których zakres napięcia wejściowego to 200-800 V. Dzieląc dolną wartość napięcia MPPt przez wyjściowe napięcie modułu (200/30=6.6) otrzymujemy informację, że minimalna liczba modułów w szeregu to 7. Maksymalną liczbę modułów obliczamy analogicznie: górną wartość napięcia MPPt dzielimy przez wyjściowe napięcie modułu (800/30=26.6) – maksymalna liczba modułów to 26.

Podsumowanie

Podsumowując, czynnikiem kluczowym w doborze paneli do falownika jest wzajemna kompatybilność oraz dopasowana charakterystyka pracy w zakresach napięcia, mocy oraz prądu. Źle dobrany falownik może doprowadzić do spadków uzysków, a co za tym idzie – wydłużenia czasu zwrotu inwestycji. •

Konfiguracja sprzętowa kontrolera PACSystems RSTi-EP. Konfiguracja komunikacji w kontrolerze

Kurs programowania PACSystems RSTi-EP CPE200

Ten artykuł jest częścią kursu programowania kontrolerów PACSystems RSTi-EP CPE200. Dowiesz się z niego, w jaki sposób dokonać konfiguracji sprzętowej swojego kontrolera PACSystem RSTI-EP. Dowiesz się także, jak prawidłowo skomunikować jednostkę centralną z oprogramowaniem narzędziowym PAC Machine Edition i wgrać jej pierwszą konfigurację do kontrolera. Cały kurs znajdziesz na stronach internetowych Poradnika Automatyka.

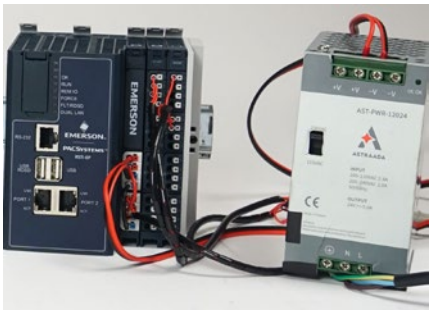
Zestaw testowy, wykorzystywany w naszym kursie, składa się z kilku elementów składowych. Są to:

- Jednostka centralna o numerze katalogowym EPSCPE205.
- Moduł wejść dyskretnych o numerze katalogowym EP-125F.
- Moduł wyjść dyskretnych o numerze katalogowym EP-225F.
- Zasilacz obiektowy Astraada o mocy 10 W.
- Układ wykonawczy – przenośnik taśmowy (opcjonalny).
- Kabel Ethernet.

Sposób podłączenia zasilania do jednostki centralnej

W pierwszym kroku podłączamy wcześniej przygotowany zasilacz Astraada według schematu i kolorów kabli jak na zdjęciu poniżej:

Kolejny krok to podłączenie kabli zasilających 24 VDC do jednostki centralnej. Koniecznie upewnij się, że zasilanie podłączasz na właściwe zaciski w sterowniku.

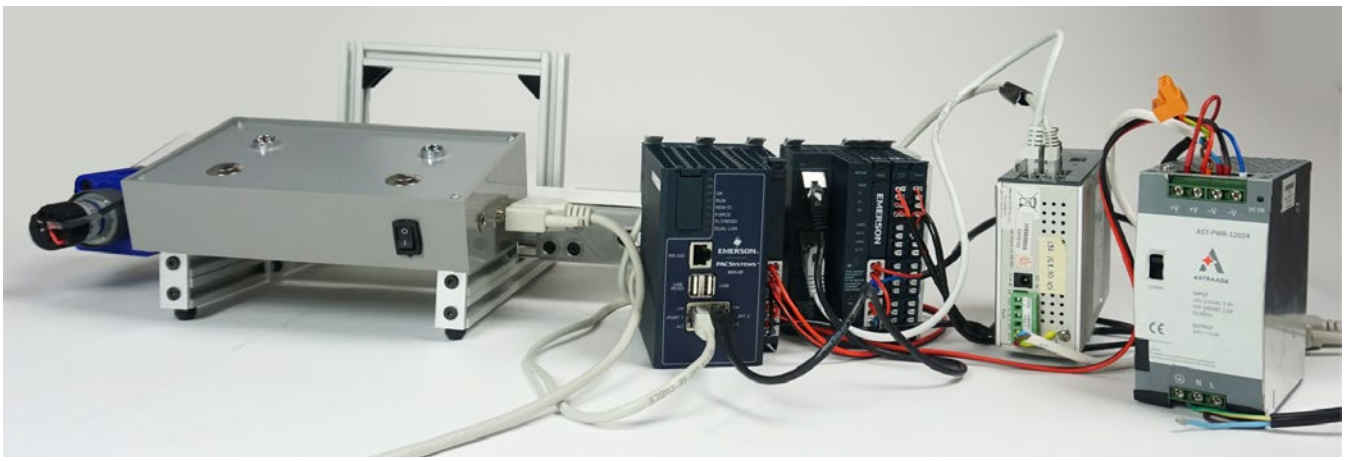


Kiedy mamy już odpowiednio zasiloną jednostkę centralną, możemy sprawdzić, czy urządzenie włącza się. Możesz zaobserwować poprawne włączenie na podstawie diody OK (święci ciągle kolorem zielonym).

Kolejnym krokiem jest podłączenie do jednostki centralnej modułów rozszerzeń. Pamiętaj, aby nie robić tego pod napięciem. Dodajemy moduły zgodnie z konfiguracją, jaką przygotowaliśmy w oprogramowaniu. Moduły łączymy poprzez zsunięcie ich ze sobą oraz osadzenie ich na szynie DIN. W tym celu wykorzystujemy klamrę montażową, która znajduje się na górnej części każdego modułu. Należy się upewnić, czy moduł po instalacji dobrze pasuje oraz odpowiednio przylega do modułu po jego lewej stronie.

Jest to ważny etap, ponieważ w przypadku braku odpowiedniego połączenia sterownik będzie generować błędy danych z powodu przerwania magistrali danych. Dodatkowo w celu zapewnienia lepszej sztywności modułów na szynie DIN można zastosować elementy blokujące przesuwanie się modułów na szynie. Tak złożony sterownik jest gotowy do konfiguracji i programowania.

Teraz przy pomocy kabla Ethernet możesz podłączyć komputer PC i sterownik PLC wykorzystując w tym celu wbudowany PORT 1 i wykonać pierwszą konfigurację wraz z testowym połączeniem. Jak to wykonać, zostało pokazane i opisane w odcinku 4 naszego kursu.



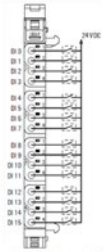
Stanowisko testowe PACSystems RSTi-EP. Źródło: ASTOR

Po wykonaniu poprzednich kroków możesz podłączyć swój zestaw testowy. W tym celu konieczne jest poznanie specyfikacji twoich modułów.

EP-125F – 16 wejść dyskretnych 24VDC; logika dodatnia – moduł ten wykorzystywany jest do wprowadzenia fizycznych sygnałów sterujących do sterownika PLC. Najczęściej wykorzystywanym standardem jest sygnał 24 VDC i dokładnie takie sygnały będziemy wykorzystywali w naszym układzie wykonawczym.

W ofercie RSTi-EP dostępne jest kilka różnych modułów wejść dyskretnych, które pozwalają na podłączania czujników 2-,3- lub 4-przewodowo. Wykorzystany moduł EP-125F pozwala podłączyć 16 czujników, z czego sygnał sterujący +24 VDC wprowadzony jest na zacisk modułu, natomiast sygnał zero z każdego czujnika podłączonego do modułu podłączamy do zacisku 0 VDC na zacisku zasilania na module PLC:

Digital Input Module EP-125F

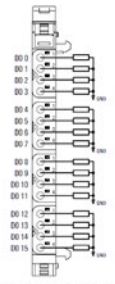


Connection Diagram EP-125F

EP-225F – 16 wyjść dyskretnych 24VDC;0,5A; logika dodatnia – moduł ten wykorzystywany jest do wyprowadzenia fizycznych sygnałów sterujących ze sterownika PLC na obiekt. Najczęściej wykorzystywanym standardem jest sygnał 24 VDC i dokładnie takie sygnały będziemy wykorzystywali w naszym układzie wykonawczym.

W ofercie RSTi-EP dostępne jest kilka różnych modułów wyjść dyskretnych, które pozwalają na podłączania czujników 2- lub 3-przewodowo. Wykorzystany przez nas moduł EP-225F pozwala podłączyć 16 czujników, z czego sygnał sterujący +24 VDC wprowadzony jest na zacisk modułu, natomiast sygnał zero z każdego elementu wykonawczego podłączonego do modułu podłączamy do zacisku 0 VDC na zacisku zasilania na module PLC:

Digital Output Module EP-225F

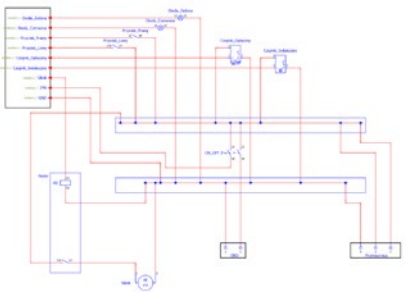


Connection Diagram EP-225F

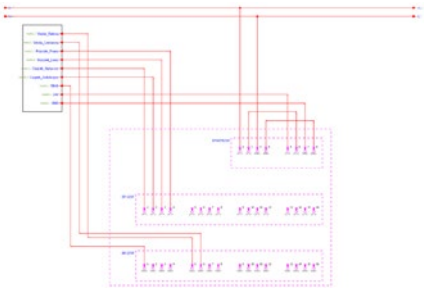
Kompletny kurs programowania kontrolerów PACSystems CPE200 znajdziesz na stronie Poradnika Automatyka:

↳ www.astor.com.pl/poradnikautomatyka/kurs-programowania-pacsystems-rsti-ep-cpe200/

Następnie według schematu oraz instrukcji poniżej podłącz kable zestawu testowego. Cały schemat jak to zrobić znajdziesz poniżej:



Schemat elektryczny przenośnika taśmowego. Źródło: ASTOR



Schemat elektryczny podpięcia sterownika z zasilaniem i układem przenośnika. Źródło: ASTOR

Uwaga! Moduły oraz wszystkie kable muszą być podłączone w sposób identyczny, jak na schemacie. W innym przypadku adresy zmiennych przypisanych w szkoleniu będą się różnić! •

AUTOR: **Mateusz Pytel**

Menedżer produktu Astraada One

mateusz.pytel@astor.com.pl

→ Tworzenie projektów w CODESYS ze sterownikami bezpieczeństwa Safety

Kurs programowania w CODESYS

Sterownik bezpieczeństwa to kluczowy element układu bezpieczeństwa w maszynie, który ma za zadanie zapewnić bezpieczeństwo użytkownikom. Jego głównym zadaniem jest przywrócenie procesu lub maszyny do stanu bezpiecznego w przypadku wystąpienia sytuacji niebezpiecznej.

» Sterownik bezpieczeństwa różni się od konwencjonalnych sterowników PLC tak pod względem sprzętu, jak i oprogramowania. Słowo kluczowe, które opisuje różnice między tymi urządzeniami, to „redundancja".

Sterowniki Safety posiadają zdublowaną architekturę sprzętową. Zarówno warstwa logiki przetwarzania sygnałów, jak i układy wejść/wyjść bezpiecznych są dwukanałowe. Sterownik Safety PLC posiada oddzielny mikroprocesor odpowiedzialny za komunikację, a także dwa redundantne układy procesorowe realizujące logikę. Zbierają one sygnały z **dwukanałowych wejść/wyjść Safety I/O**, wykonują obliczenia i porównują je wzajemnie. W przypadku wykrycia niezgodności lub uszkodzenia któregoś z układów, proces natychmiast zostaje przekierowany do stanu bezpiecznego. Dwukanałowość układów Safety I/O zapewnia, że sygnał wejściowy zostanie poprawnie przetworzony, a sygnał wyjściowy pojawi się na wyjściu nawet w przypadku uszkodzenia jednego z kanałów.

Sterownik bezpieczeństwa Astraada SC-1000 oraz Astraada SC-I/O, źródło: ASTOR

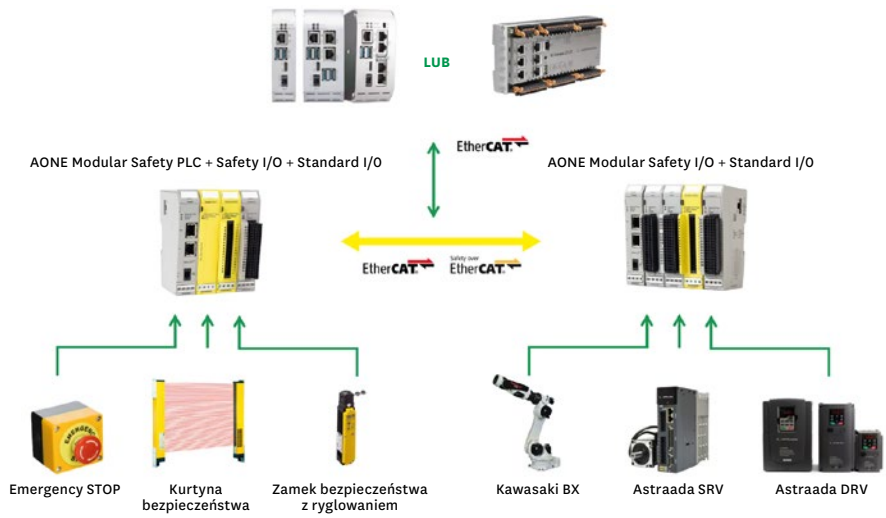
Rozbudowane funkcje autodiagnostyki wykrywają wszelkie możliwe usterki wewnętrzne – zarówno sprzętu, jak i oprogramowania, dzięki czemu awaria sterownika nie prowadzi do sytuacji „niebezpiecznej". Sterowniki Safety PLC posiadają również ważne zabezpieczenia przed nieautoryzowanym dostępem. Są one realizowane poprzez wielopoziomowy dostęp chroniony hasłem oraz śledzenie zmian w programie Safety. Sterowniki Safety przechodzą rygorystyczne testy podczas procesu certyfikacji, mające na celu eliminację błędów zarówno w warstwie sprzętowej, jak i oprogramowaniu.

Sterownik bezpieczeństwa jest urządzeniem typu Slave – w systemie, który kontrolowany jest przez jednostkę nadrzędną. Najczęściej jest nią zwykły sterownik PLC. Do opracowania tego odcinka kursu użyto **sterownika bezpieczeństwa Astraada SC-1000**, a komunikacja pomiędzy sterownikami realizowana jest za pomocą protokołu **EtherCAT**. Natomiast komunikacja bezpieczeństwa pomiędzy sterownikiem Safety a układami wejść/wyjść Safety realizowana jest za pomocą **certyfikowanego protokołu bezpieczeństwa FSoE (*Fail Safe over EtherCAT*)**, dla którego EtherCAT jest medium komunikacyjnym.

Sterownik bezpieczeństwa Astraada, podobnie jak sterowniki Astraada One, programuje się w **środowisku CODESYS**, co ułatwia szybkie zbudowanie spójnego układu bezpieczeństwa. Programowanie funkcji bezpieczeństwa odbywa się za pośrednictwem certyfikowanego rozszerzenia Safety w tym oprogramowaniu. Sterownik Safety korzysta z biblioteki **PLCopen Safety**, która oferuje certyfikowane bloki funkcyjne dedykowane do budowania programów bezpieczeństwa. Ważną zaletą jest dwukierunkowa wymiana danych pomiędzy jednostką główną oraz jednostką Safety, dzięki czemu możliwa jest wizualizacja stanu bezpieczeństwa maszyny oraz wzajemne oddziaływanie programów.

Przygotowanie środowiska do utworzenia projektu Safety

Aby móc dodać oraz programować sterownik bezpieczeństwa Astraada, musisz



Architektura systemu bezpieczeństwa w oparciu o duet Astraada Safety PLC i Astraada One PLC. Źródło: ASTOR

posiadać odpowiednią wersję środowiska CODESYS na swoim komputerze. Rekomendowaną wersją oprogramowania jest wersja 3.5 SP16 Patch 4. Jeśli chciałbyś zacząć pracę ze sterownikiem bezpieczeństwa Astraada na innej wersji CODESYS, najpierw skonsultuj tą kwestię z Działem Pomocy Technicznej ASTOR.

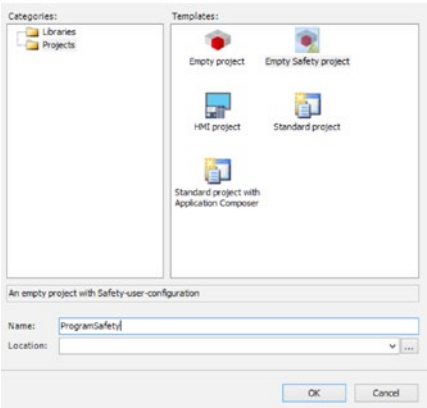
Dodatkowo oprogramowanie wymaga specjalnych plików sprzętowych **Device Repository** oraz **Package Manager**, które można uzyskać, kontaktując się z Działem Pomocy Technicznej ASTOR.

Odpowiednio przygotowane środowisko wraz ze sterownikiem powinno posiadać:

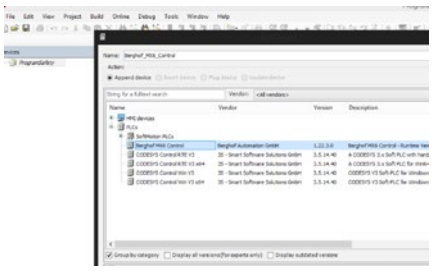
- Rozszerzenie Safety (E-IO_Safety_Extension_V1.5.0.0_for_CODESYS_V3.5.14.40) w narzędziu Package Manager.
- Firmware w wersji 1.22.3 zainstalowany w sterowniku nadrzędnym.
- Target w projekcie w wersji 1.22.3.
- Odpowiednie pliki dotyczące modułów Safety za pomocą narzędzia Device Repository.

Dodanie sterownika bezpieczeństwa do projektu CODESYS

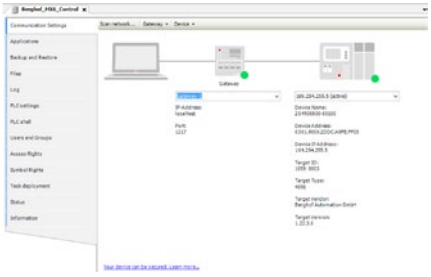
Jeśli wszystkie wyżej wymienione punkty zostały spełnione, możesz przejść do utworzenia projektu Safety. Aby to zrobić, wybierz opcję **New Project**, a następnie **Empty Safety Project** oraz nazwij swój projekt i kliknij przycisk **OK**:



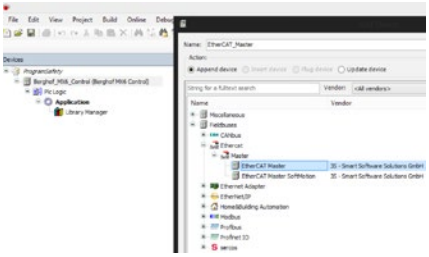
W taki sposób utworzyliśmy nowy projekt Safety. Domyślnie jest on pusty, zatem musisz dodać nowe urządzenie do swojego projektu. Kliknij prawym przyciskiem myszy na jedyny utworzony segment w drzewku projektowym i wybierz **Add Device**. Z listy należy wybrać sterownik nadrzędny, który jest podłączony do sterownika Safety:



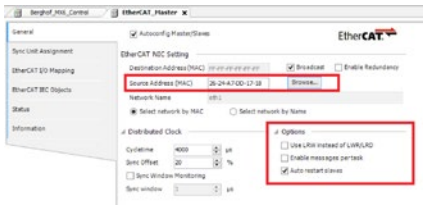
Po dodaniu sterownika kliknij na niego dwukrotnie i w menu **Communication Settings** wpisz jego adres IP oraz zatwierdź klawiszem ENTER, aby połączyć się ze sterownikiem:



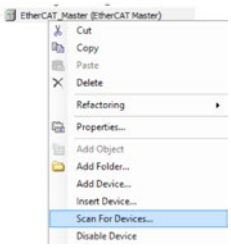
Po dodaniu sterownika czas na dodanie i konfigurację komunikacji z sterownikiem bezpieczeństwa. W tym przypadku będzie to wykonywane z wykorzystaniem protokołu EtherCAT, za pomocą Buscouplera Astraada. Zacznij od dodania EtherCAT Master do projektu. Wybierz prawym przyciskiem myszy sterownik nadrzędny, wybierz opcję **Add Device** i dodaj **EtherCAT Master**:



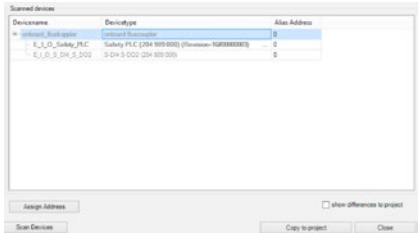
Następnie skonfiguruj połączenie EtherCAT – poprzez kliknięcie na **EtherCAT Master** i ustawienie adresu MAC wykorzystywanego portu (w przykładowym sterowniku jest to **eth1**), uprzednio ustawiając port RJ45 w sterowniku nadrzędnym do komunikacji za pomocą tego protokołu, co można zrobić z poziomu Webservera. Warto także rozwinąć segment **Options** i zaznaczyć opcję **Auto restart slaves** – umożliwi to automatyczne nawiązywanie komunikacji z urządzeniami na wypadek utraty komunikacji:



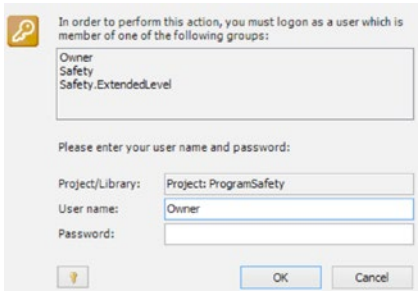
Dzięki tej konfiguracji dostępna będzie opcja **Scan for Devices**, która automatycznie wykryje połączone ze sterownikiem urządzenia Slave, które wykorzystują protokół EtherCAT, czyli w tym przypadku Buscoupler oraz sterownik bezpieczeństwa. Opcję tę możesz znaleźć poprzez kliknięcie prawym przyciskiem myszy na **EtherCAT Master** w drzewku projektowym:



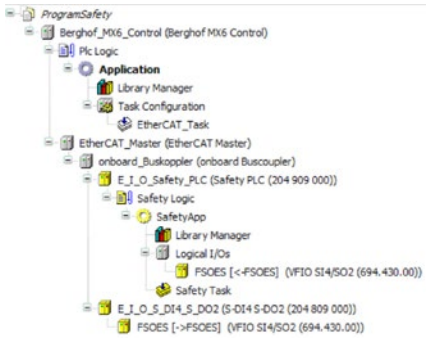
Po krótkim czasie zostanie wyświetlona lista podłączonych urządzeń. Aby dodać wybrane urządzenia do projektu, należy przytrzymać lewy klawisz **CTRL** na klawiaturze i jednocześnie kliknąć lewym przyciskiem myszy na poszczególne urządzenia. Po zaznaczeniu odpowiednich urządzeń, należy wybrać opcję **Copy to project**:



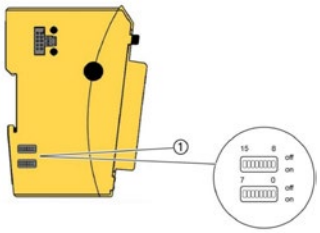
Aplikacja poprosi o podanie loginu i hasła. Najwyższy poziom dostępu oferuje login **Owner**, który standardowo nie ma zaprogramowanego żadnego hasła. W związku z tym należy podać sam login i potwierdzić klawiszem **OK**:



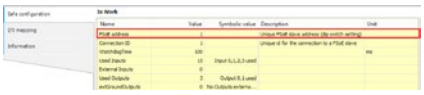
Drzewko zostanie automatycznie rozbudowane o urządzenia Safety wraz z bibliotekami i opcjami, umożliwiającymi stworzenie programu Safety i wgranie go do urządzenia. Jeśli zostały dodane same urządzenia, należy dodać pozostałe części projektu samodzielnie, aby drzewko projektu wyglądało jak na zdjęciu poniżej.



Przy korzystaniu z dodatkowych modułów Safety I/O należy sprawdzić, czy posiadają one poprawnie zdefiniowany adres ID sieci FSoE. Aby to zrobić, należy zweryfikować stan przełączników DIP na wewnętrznej stronie modułu I/O. Wszystkie przełączniki fabrycznie powinny być ustawione na pozycję **OFF**. Należy wybrać odpowiedni adres FSoE, zgodnie z wymaganiami. Na przykład, jeśli moduł I/O ma mieć adres 1, należy przestawić drugi przełącznik z prawej strony dolnego segmentu w tryb **ON**.

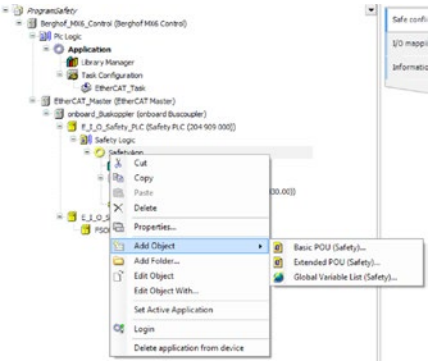


Następnie przejdź do drzewa projektu i dwukrotnie kliknij dodany moduł I/O w segmencie **Logical I/Os**. W efekcie wyświetli się menu konfiguracyjne modułu I/O. W tym miejscu ważne jest, aby upewnić się, czy adres Slave (adres podrzędny) zgadza się z fizycznym ustawieniem przełączników. Należy sprawdzić, czy adres w menu konfiguracyjnym odpowiada rzeczywistemu stanowi przełączników.



Konfiguracja Safety I/O, źródło ASTOR

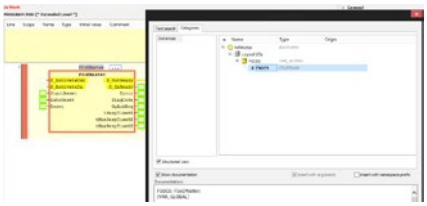
Jeżeli wystąpi niezgodność, kompilator wykryje błąd i uniemożliwi wgranie programu. Następnym krokiem jest dodanie obiektu **POU** (Program Organization Unit), w którym można zapisać program w języku Safety FBD. Aby to zrobić, kliknij prawym przyciskiem myszy na **SafetyApp** i rozwiniętą opcję **Add Object**. Masz do wyboru dwa rodzaje obiektów POU: Basic i Extended. Obiekt **Basic** oferuje mniejszą liczbę obsługiwanych funkcji i rodzajów zmiennych w porównaniu do obiektu **Extended**. Ponadto, można ograniczyć dostęp do tych dwóch obiektów, tak aby zalogowany użytkownik miał dostęp tylko do określonego typu. W tym przykładzie wybierzemy obiekt Extended:



Programowanie sterownika bezpieczeństwa

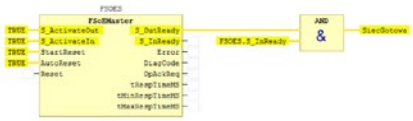
Rozpoczynając tworzenie programu Safety ważne jest, aby w pierwszej kolejności dodać blok **FSoEMaster**. Ten blok ma za zadanie monitorować status połączenia FSoE (FailSafe over EtherCAT) oraz diagnozować wejścia/wyjścia, decydując o kontynuacji pracy programu. Jeśli nie jest on dostępny w Toolboxie, można przeciągnąć dowolny inny blok do programu, a następnie dwukrotnie kliknąć na jego nazwę i ręcznie wpisać **FSoEMaster**. Po zatwierdzeniu klawiszem **ENTER**, blok zostanie odpowiednio zmodyfikowany.

W bloku FSoEMaster istotną rolę odgrywa zmienna, którą ten blok definiuje. Nie może to być dowolna zmienna, ale specjalnie przygotowana zmienna powiązana z modułem I/O. Aby skonfigurować odpowiednią zmienną, należy kliknąć na trzy kropki powyżej bloku i wybrać **SafeApp → Logical I/Os → FSOES → FSOES**. Dzięki temu blok zostanie skonfigurowany wraz z połączonym modułem.



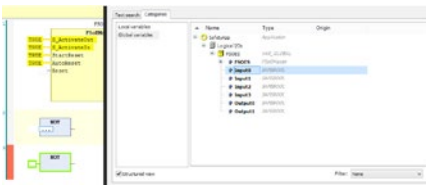
Aby zapewnić poprawne działanie bloków Safety, konieczne jest posiadanie zmiennej, która pozwoli na ich aktywację. Każdy blok funkcyjny Safety (z wyjątkiem FSoEMaster, który działa ciągle) posiada wejście o nazwie Active. Dlatego też najlepiej skorzystać z funkcjonalności diagnostycznej bloku FSoEMaster i zezwolić na aktywację pozostałych bloków tylko wtedy, gdy wejścia i wyjścia przejdą pomyślnie test diagnostyczny.

Aby stworzyć taką zmienną, należy przypisać wartość **True** do wejść **S_ActiveOut** oraz **S_ActiveIn**, co uruchomi diagnostykę fizycznych wejść i wyjść. Należy także przypisać wartość **True** do wejść **StartReset** oraz **AutoReset**, które umożliwią ciągłą i automatyczną pracę bloku. Następnie, można skorzystać z wyjść **S_OutReady** oraz **S_InReady**, które informują o poprawnym (wartość **True**) lub niepoprawnym (wartość **False**) działaniu I/O. Wyjścia te można połączyć za pomocą bloku **AND**, co pozwoli zdefiniować zmienną, która przyjmie wartość **True** tylko wtedy, gdy zarówno wejścia, jak i wyjścia pomyślnie przejdą test diagnostyczny.



Kolejnym krokiem jest kontynuowanie tworzenia programu. W tym przykładzie zostanie zdefiniowany przycisk o dwóch wejściach typu **NC** (Normally Closed), który aktywuje wyjście oznaczone jako **Output 1**.

Aby uzyskać bezpośrednie odwołanie do fizycznych wejść i wyjść modułu I/O, należy przejść do segmentu **Global variables** i rozwinąć drzewko opcji. Tam można znaleźć odpowiednie zmienne odnoszące się do fizycznych wejść i wyjść, z którymi można dalej pracować w programie:

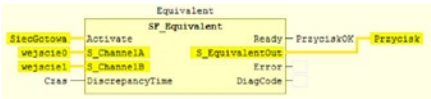


Aby przetworzyć dwa sygnały wejściowe na jeden sygnał wyjściowy, można skorzystać z bloków **SF_Equivalent** (równorzędne) lub **SF_Antivalent** (przeciwnorzędne), w zależności od rodzaju styków w przycisku. W tym przykładzie styki są tego samego rodzaju (NC – Normally Closed), dlatego użyjemy bloku SF_Equivalent.

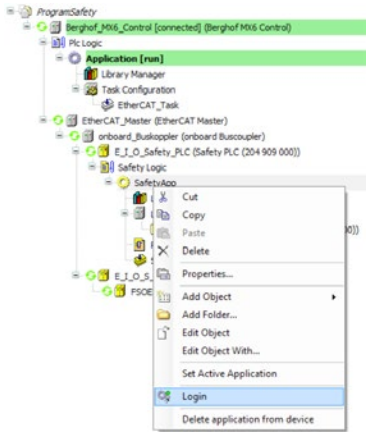
Aby poprawnie skonfigurować blok SF_Equivalent, należy:

- Na wejściu **Active** podać zmienną, która aktywuje działanie bloku. W tym przykładzie jest to zmienna **SiecGotowa**, którą wcześniej przygotowaliśmy.
- Podłączyć sygnały wejściowe z przycisku do wejść **S_Channel1A** oraz **S_Channel1B**.
- Stworzyć zmienną **Czas**, w której zdefiniujemy maksymalny czas, w jakim oba sygnały mają zmienić stan na **True**. W tym przypadku styki działają w ramach jednego przycisku, więc sygnały prawdopodobnie zmienią się niemal jednocześnie, dlatego ten czas może być krótki.
- Zdefiniować zmienną przy wyjściu **Ready**, która informuje o gotowości bloku do działania, oraz zmienną przy wyjściu **S_EquivalentOut**, która będzie główną zmienną wyjściową.

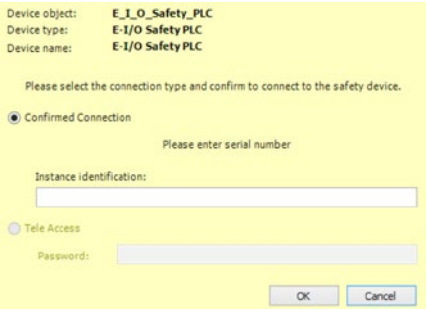
Dzięki tak skonfigurowanemu blokowi będziemy w stanie przetworzyć dwa sygnały wejściowe z przycisku na jeden sygnał wyjściowy:



Po skonfigurowaniu programu można przejść do procesu wgrywania programu. Pierwszym krokiem jest nawiązanie komunikacji z głównym sterownikiem i zalogowanie się do niego, a następnie wgranie programu. Poprawne nawiązanie komunikacji będzie sygnalizowane przez zielone strzałki, które pojawią się po przejściu sterownika w tryb **RUN**. Następnym krokiem jest zalogowanie się bezpośrednio do sterownika Safety. Aby to zrobić, należy kliknąć prawym przyciskiem myszy na **SafetyApp** i wybrać opcje **Login**:



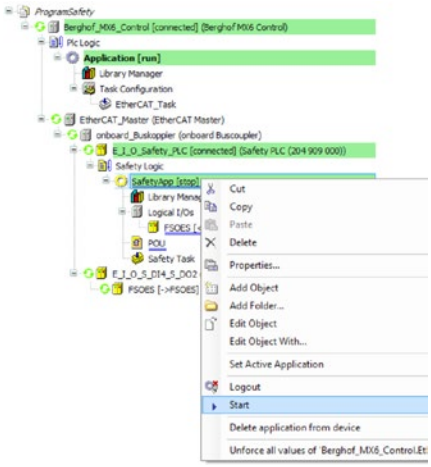
Aplikacja poprosi o weryfikację logowania poprzez podanie numeru seryjnego sterownika Safety. Należy taki numer podać i wcisnąć **OK**:



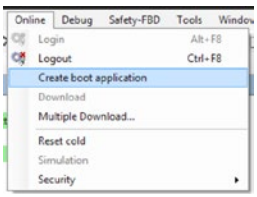
Następnie zostanie wyświetlony komunikat informujący, że wgrana aplikacja różni się od obecnie zainstalowanej w sterowniku. Po potwierdzeniu tego komunikatu, sterownik zostanie przełączony w tryb testowy, umożliwiający wgranie nowej aplikacji i przeprowadzenie fizycznego testu na sprzęcie.

Ostatnim komunikatem będzie prośba o podanie hasła. Domyślnie hasło nie jest ustawione, więc wystarczy kliknąć przycisk **OK**.

Po wgraniu aplikacji należy przełączyć sterownik Safety w tryb RUN, klikając prawym przyciskiem myszy na ikonę **SafetyApp** i wybierając opcję **Start**. W tym momencie można przeprowadzić test funkcjonalności aplikacji.



W celu zapewnienia trwałości wgranej aplikacji w sterowniku Safety, po zalogowaniu się do niego i przeprowadzeniu testu poprawności działania konieczne jest przygotowanie pliku **Boot**. Aby to zrobić, kliknij prawym przyciskiem myszy na ikonę **SafetyApp** i wybierz opcję **Set Active Application**, a następnie udaj się do lewego górnego rogu ekranu, rozwiń opcję **Online** i wybierz **Create boot application**. Zostanie utworzony plik Boot, który zapewni przywrócenie wgranej aplikacji po wylogowaniu się z sterownika.



Po wylogowaniu się z sterownika oprogramowanie wyświetli pytanie, czy sterownik powinien zostać zrestartowany i uruchomiony z aktualną wersją aplikacji boot, która została wgrana do pamięci. Konieczne jest potwierdzenie tego komunikatu. Od tego momentu sterownik będzie działał z zainstalowaną aplikacją i będzie realizować jej funkcje zgodnie z programem, który został napisany. •

Kompletny kurs programowania CODESYS znajdziesz na stronie Poradnika Automatyka:

↳ www.astor.com.pl/poradnikautomatyka/kurs-programowania-w-codesys/

Komunikacja EtherCAT – konfiguracja w środowisku CODESYS

Kurs obsługi i konfiguracji serwonapędów Astraada SRV

Ten artykuł jest fragmentem kursu obsługi i konfiguracji serwonapędów Astraada SRV. W tym odcinku omówimy pracę w trybie sterowania prędkością oraz pozycją w środowisku CODESYS na podstawie prostej aplikacji realizującej wymienione tryby działania urządzenia. Cały kurs znajdziesz na stronach internetowych Poradnika Automatyka.

AUTOR: **Marcin Ryznar**

Asystent ds. obsługi sklepu internetowego

marcin.ryznar@astor.com.pl

» Odcinek został poświęcony sposobowi działania serwonapędu Astraada SRV w wersji EtherCAT bez dodatkowych licencji. Na samym początku przedstawię rozwiązanie, które pozwoli Ci skonfigurować i skomunikować oprogramowanie CODESYS z serwonapędem Astraada SRV poprzez sieć EtherCAT. Następnie poznasz tajniki parametrów umożliwiających pracę w wybranym trybie sterowania. Taki zasób wiedzy pozwoli zrozumieć ideę tworzenia aplikacji.

Dzięki komunikacji EtherCAT informacje przekazywane są do wielu urządzeń jednocześnie. Dane przesyłane są za pomocą kart sieciowych oraz okablowania, a sam protokół bazuje na architekturze Master – Slave. Masterem nazywamy urządzenie nadrzędne – odpowiedzialne za wysyłanie komunikatów, natomiast Slave to jednostka podrzędna – odbierająca informacje nadawane przez master.

Przygotowanie serwonapędu Astraada SRV do komunikacji w protokole EtherCAT

Przed przystąpieniem do konfigurowania serwonapędu zaleca się przywrócenie jego ustawień fabrycznych. Jest to realizowane poprzez wpisanie wartości **1** do rejestru **P4.92** i ponowne załączenie zasilania.

Serwonapęd Astraada SRV domyślnie nie jest skonfigurowany do komunikacji za pośrednictwem sieci EtherCAT. Należy więc uaktywnić w nim opcję komunikacji w tym protokole.

1. Ustaw tryb pracy serwonapędu na sterowanie za pomocą sieci EtherCAT. W tym celu do parametru **P0.03** wpisz wartość **8**. Po zmianie tego parametru wyłącz i załącz zasilanie wzmacniacza.
2. Ustaw typ synchronizacji za pomocą sieci EtherCAT w parametrze **P4.08** na
   - **0** (Free-Run, tj. praca bez synchronizacji)
   - lub **1** (DC Sync0, czyli praca z synchronizacją lokalnych zegarów poszczególnych urządzeń podrzędnych)
3. Skonfiguruj okres synchronizacji EtherCAT, tj. czas wymiany danych z użyciem tej sieci. W tym celu wpisz odpowiednią wartość do parametru **P4.07**:
   - Wartość **0** oznacza 250 µs,
   - Wartość **1** oznacza 500 µs,
   - Wartość **2** oznacza 1 ms,
   - Wartość **3** oznacza 2 ms.
4. W parametrze **P4.09** ustaw czas **Fault Detection Time**, tzn. czas timeout, dla komunikacji EtherCAT (np. wpisz 100 ms). Posłuży on do wykrywania faktu utraty komunikacji sieci.

Upewnij się, że w parametrze **P0.00** został skonfigurowany taki model silnika, jaki rzeczywiście dołączony jest do serwowamacniacza. Numer modelu silnika jest nadrukowany na silniku. Po zmianie modelu silnika należy wyłączyć i włączyć zasilanie wzmacniacza.

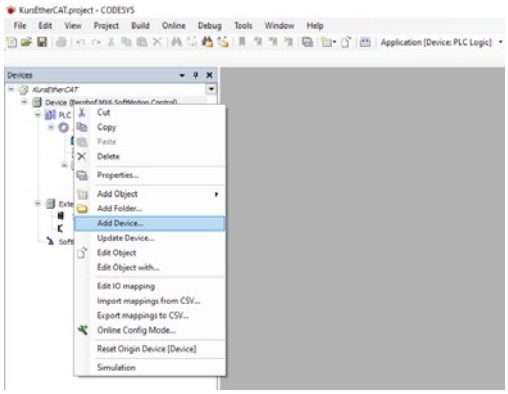
UWAGA! Sterownik Astraada One musi być połączony ze wzmacniaczem serwonapędu Astraada SRV przy użyciu pierwszego (tj. górnego) portu EtherCAT w tym wzmacniaczu – gniazdo CN3.

Konfigurowanie komunikacji EtherCAT w oprogramowaniu CODESYS

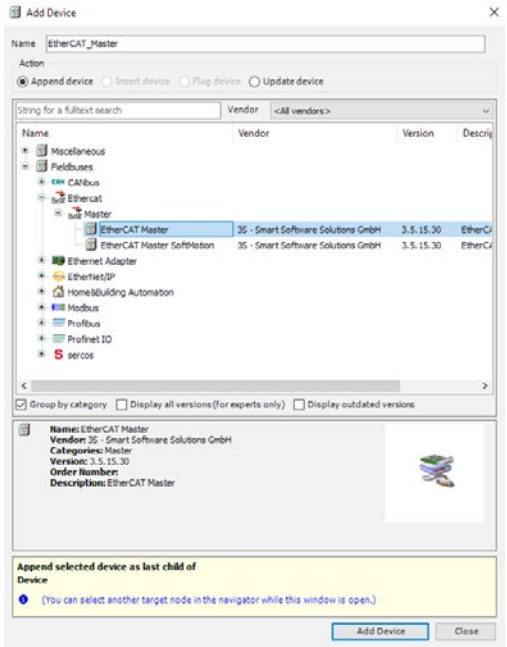
Pierwszym krokiem, od którego powinniśmy zacząć, jest stworzenie nowego projektu w środowisku CODESYS. Następnie dodaj do niego swój sterownik i wybierz język **Ladder Logic Diagram** (LD). Język drabinkowy nie jest wyborem obligatoryjnym, w późniejszym etapie pisania aplikacji możesz go zmienić. Co więcej, Twoja aplikacja może zostać napisana w kilku językach jednocześnie.

Pamiętaj o dodaniu pliku deskrypcyjnego do obsługi serwonapędów Astraada SRV w celu poprawnego skonfigurowania połączenia. Jeżeli jeszcze nie konfigurowałeś serwonapędów Astraada SRV w oprogramowaniu CODESYS wybierz polecenie **Tool → Device Repository** i wskaż lokalizację pobranego pliku (np. Astraada_SRV_CoE_V106.xml).

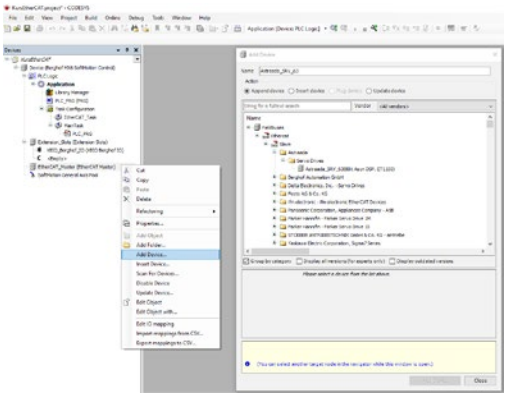
Następnie w celu uaktywnienia w sterowniku Astraada One obsługi protokołu EtherCAT kliknij prawym przyciskiem myszy w drzewku projektu na **Device** i zaznacz polecenie **Add Device**.



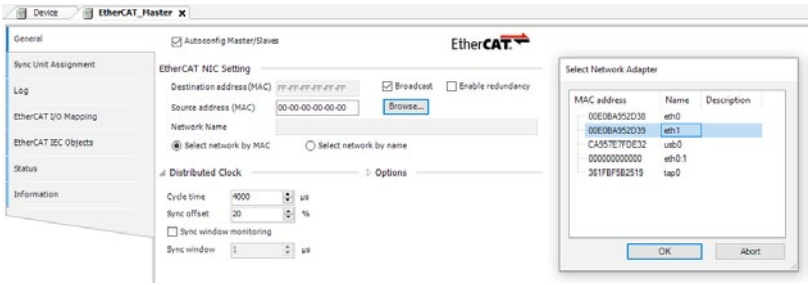
W następnej kolejności w polu **Vendor** wybierz **<All vendors>** i rozwiń listę, która pozwoli Ci przejść do **EtherCAT Master**. Zatwierdź wybór poprzez dwukrotne kliknięcie lewym przyciskiem myszy lub dzięki przyciskowi **Add Device**.



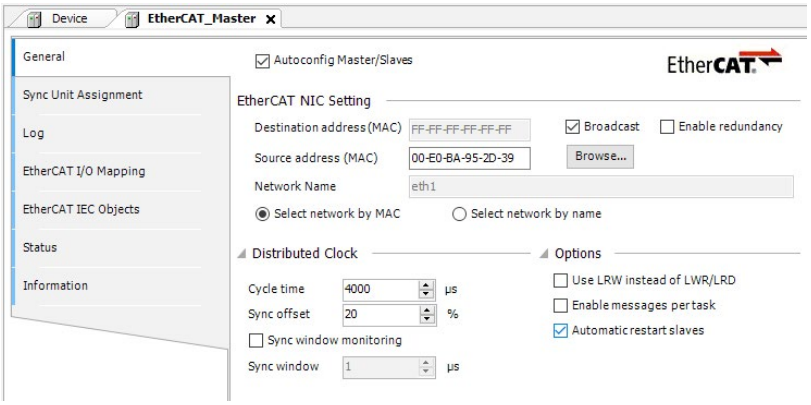
Podobnie jak w punkcie 2 kliknij opcję **Add Device**, jednak po wcześniejszym wybraniu **EtherCAT_Master**. Po chwili ujrzysz okno, w którym możemy wybrać nasze urządzenie podrzędne, jakim jest **serwonapęd serii Astraada SRV-63**. Dodaj je do projektu.



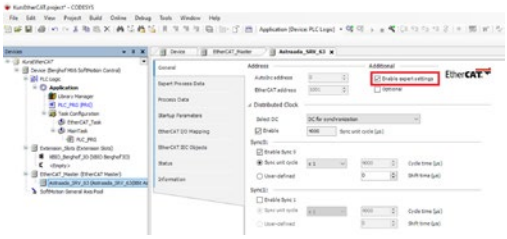
W kolejnym kroku musimy zdefiniować port w sterowniku, który odpowiada za pracę w roli urządzenia nadrzędnego – Master sieci EtherCAT. Można wybrać go za pomocą adresu MAC portu lub nazwy karty sieciowej. Dokonanie wyboru poprzez nazwę karty sieciowej jest powszechnym i mniej problematycznym sposobem. W tym ćwiczeniu używamy sterownika, gdzie **port eth1** możemy zdefiniować jako Master w sieci EtherCAT, więc wybierając przycisk **Browse....** W oknie **Select Network Adapter** w kolumnie **Name** zaznaczamy **eth1.**



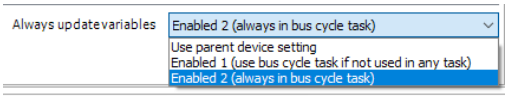
Jak możesz zauważyć, w polu **Source Address (MAC)** został dodany adres MAC wybranego przez nas portu komunikacyjnego sterownika Astraada One. Z kolei gdy zaznaczymy opcję **Auto restart slaves**, sterownik samoczynnie zacznie ponawiać próby komunikacji z serwonapędem w przypadku niepożądanych sytuacji, takich jak np. rozłączenie na moment kabla komunikacyjnego EtherCAT.



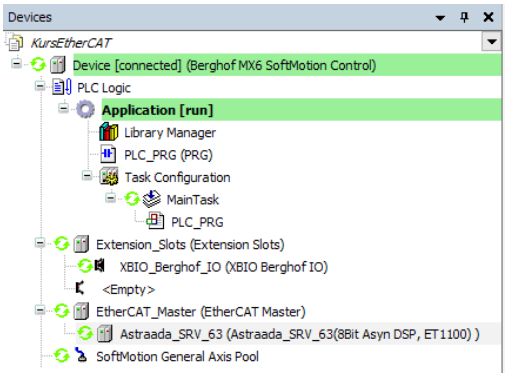
Przechodzimy następnie do konfiguracji wcześniej dodanego urządzenia podrzędnego. Wybieramy więc **Astraada_SRV_63** z drzewka projektu i w rubryce **Additional** zakładki **General** zaznaczamy opcję **Enable Expert Settings**.



Znajdując się w miejscu do konfiguracji naszego urządzenia podrzędnego przechodzimy do zakładki **EtherCAT I/O Mapping** i zaznaczamy opcję służącą do śledzenia zmiennych nieużywanych w programie. Dzięki niej przeprowadzamy testy serwonapędu, zanim zostanie napisany program sterujący z ich użyciem. W prawym dolnym rogu wybieramy, więc opcję **Enabled 2.**



Świetnie, w tym momencie jesteśmy gotowi, by sprawdzić status komunikacji EtherCAT. Poprawna komunikacja z serwonapędem za pośrednictwem sieci EtherCAT będzie sygnalizowana następującymi ikonkami:

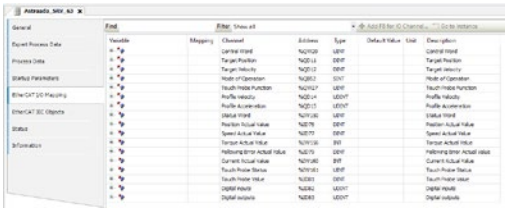


W przypadku niepowodzenia i wyświetlenia pomarańczowego trójkąta oznaczającego brak komunikacji, zweryfikuj poprawność konfiguracji serwowzmacniacza w protokole EtherCAT.

Dodawanie parametrów sterujących

Wchodząc poprzez drzewko programu w **Astraada_ARV_63**, a następnie w **zakładkę EtherCAT I/O Mapping** mamy dostęp do parametrów dostarczonych przez bibliotekę serwonapędu. Musimy mieć na uwadze, iż ilość danych wymienianych z serwonapędem jest ograniczona i pozwala na dodanie jedynie jednego parametru wyjściowego służącego do zapisu. Dlatego pamiętaj, aby rozważyć współczynniki, które będą niezbędne do użycia w danej aplikacji i ewentualnie usunąć zbędne z listy.

Podstawowa lista parametrów wygląda w następujący sposób:

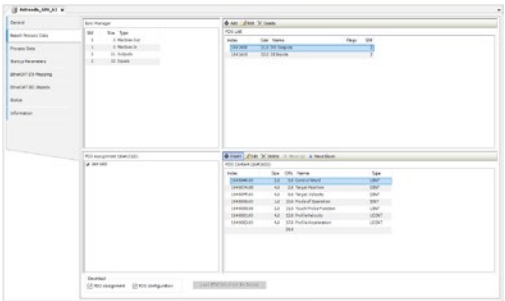


Może się okazać jednak, że na wyświetlanej liście nie ma wszystkich elementów. Z reguły dodaje się ograniczenie momentu siły (**Max Torque**), a usuwa zatrzaskiwanie pozycji (**Touch Probe Function**). W tym przypadku pokażę Ci, jakie działania przeprowadzić, aby dodać interesujące nas zmienne, które będą wymieniane między sterownikiem a serwonapędem.

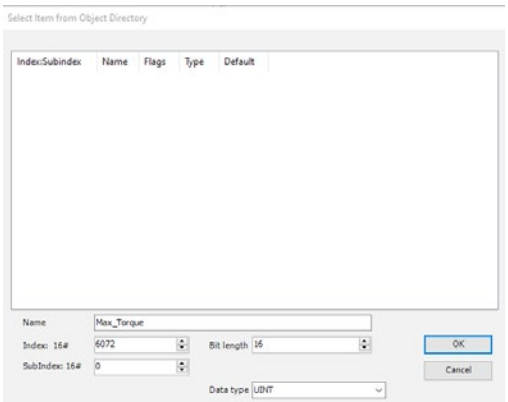
W celu dodania parametru do listy, należy wykonać następujące operacje:

1) Wyłączamy tryb komunikacji ze sterownikiem Astraada One w środowisku CODESYS za pomocą przycisku **Logout**:

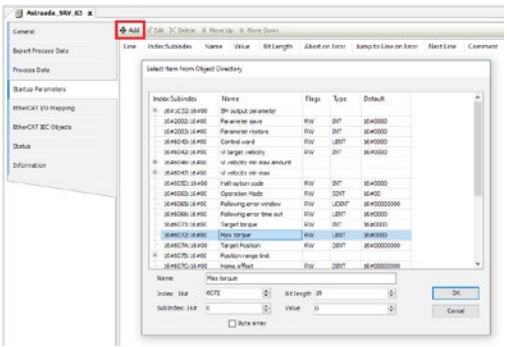
2) Wchodzimy w ustawienia urządzenia podrzędnego, a dokładniej w zakładkę **Expert Process Data.** W oknie **PDO List** (Process Data Objects) należy wybrać lewym przyciskiem myszy indeks **16#1600** (DO Outputs). Dzięki temu mamy możliwość dodania nowej zmiennej w polu **PDO Content**. Z kolei w tym polu klikając lewym przyciskiem myszy w ikonę **Insert** spowodujemy otwarcie okna, gdzie można dodać nową zmienną. Istotnym faktem jest to, że do serwowzmacniaczy możemy dodać maksymalnie 10 parametrów.



3) W oknie wpisujemy nazwę nowej zmiennej, jej adres w formacie szesnastkowym oraz wybieramy typ. Za przykład posłuży inkrementacja ograniczenia momentu obrotowego dla serwonapędu. W przypadku nowszej serii SRV-64 zadanie to jest ułatwione, ponieważ lista jest automatycznie wypełniona.



4) Jeśli chciałbyś odnaleźć adresy zmiennych, pozostań w oknie **Astraada_SRV_63**. W zakładce **Startup Parameters,** klikając przycisk **„Add",** możesz podejrzeć adresy i typy zmiennych przekazywane za pośrednictwem sieci EtherCAT do serwonapędu Astraada SRV.



Jak sprawdzić status urządzenia i jak wysyłać polecenia sterujące do serwonapędu?

Status urządzenia możemy podglądać w parametrze **Status Word (0x6041).** Natomiast w celu wymuszenia działania na stan maszyny sterującej, wykorzystujemy przede wszystkim zadane przez nas polecenia w rejestrze kontrolnym **Control Word (0x6040).**

Opis słowa statusowego (STATUS WORD, 0x6041)

Znaczenie poszczególnych bitów jest następujące:

NUMER BITU	OPIS	SPOSÓB UŻYCIA BITU
0	**Ready to switch on**	M
1	**Switched on**	M
2	**Operation enabled**	M
3	**Fault**	M
4	**Voltage enabled**	M
5	**Quick stop**	M
6	**Switch on disabled**	M
7	**Warning** – ostrzeżenie np. o przegrzaniu	O
8	Zarezerwowany dla producenta (**Manufacture specific**)	O
9	**Remote** – sterowanie zdalne po sieci EthetCAT	M
10	**Target reached** – zadana pozycja lub prędkość została osiągnięta	M
11	**Internal limit active** – aktywne ograniczenie wewnętrzne serwonapędu jak np. najechanie na krańcówki lub osiągnięcie zadanego momentu siły	M
12, 13	Zależne od trybu pracy: Bit 12 przy sterowaniu pozycją oznacza potwierdzenie otrzymania nowej wartości pozycji zadanej (**Setpoint acknowledge**), a przy procedurze kalibracji (Homing) świadczy o zakończeniu kalibracji. Bit 13 informuje o wystąpieniu błędu (**lag/following error**)	O
14, 15	**Manufacture specific** – Zarezerwowane dla producenta	O

Użycie opisanych bitów może być następujące:

- O: użycie opcjonalne,
- M: bit musi być użyty.

Opis słowa kontrolnego (CONTROL WORD, 0X6040)

Znaczenie bitów w słowie kontrolnym jest następujące:

15 (MSB)	...11	10	9	8	7	6	5	4	3	2	1	0 (LSB)
Bity specyficzne dla producenta		Zarezerwowane		Halt	Fault Reset	Operation Mode Specific			Enable Operation	Quick Stop	Enable Voltage	Switch On
O		O		O	M	O			M	M	M	M

Użycie opisanych bitów może być następujące:

- O: użycie opcjonalne,
- M: bit musi być użyty.

W opisie słowa kontrolnego musimy skupić się głównie na 5 pierwszych bitach zapisanych w rejestrze, z czego 4 muszą być zawsze używane. Poniżej przedstawiam Ci legendę, dzięki której zrozumiesz znaczenie przypisywanych bitów. Zwróć uwagę na pogrubioną czcionkę.

BIT	PEŁNIONA FUNKCJA
Switch On	**Załączenie serwonapędu**
Enable Voltage	**Załączenie obwodu zasilania dla serwonapędu**
Quick Stop	**Szybkie zatrzymanie (hamowanie dynamiczne)**
Enable Operation	**Zezwolenie na pracę serwonapędu**
Operation Mode Specific	**Bity poleceń zależne od skonfigurowanego trybu pracy (zobacz opis w dalszej części). Tryb pracy definiuje się w rejestrze Mode of Operation (0x6060); wartości do wpisania do tego rejestru podane są w punktach opisujących poszczególne tryby pracy.**
Fault Reset	Kasowanie błędu
Halt	Polecenie zatrzymania z hamowaniem dynamicznym

Praca w trybie sterowania pozycją

Ten rodzaj sterowania pozwala osiągnąć zadaną pozycję na podstawie przypisanej prędkości ruchu, przyspieszenia oraz zdefiniowanego momentu siły. Przedstawię Ci krok po kroku, jakie działania musisz przeprowadzić, aby poprawnie sterować pracą w trybie pozycji.

Swoją uwagę skupimy głównie na następujących rejestrach, którym przypisałem nazwy w celu łatwiejszej identyfikacji:

Variable	Mapping	Channel
Ograniczenie_Siły		Max_Torque
		Control Word
Pozycja_Ruchu		Target Position
		Target Velocity
Tryb_Pracy		Mode of Operation
		Touch Probe Function
Predkosc_Ruchu		Profile Velocity
Przyspieszenie		Profile Acceleration

Połącz się ze sterownikiem i przejdź do zakładki **EtherCAT I/O Mapping** w Astraada_SRV_63. Wartości wpisujemy w kolumnę **Prepared Value**, a chcąc je wpisać do sterownika, należy nacisnąć przyciski Ctrl + F7. Chcąc wykonać *force* naciśnij przycisk F7.

Następnie ustawiamy **tryb pracy**, czyli parametr **Mode of Operation (0x6060)**, na wartość **1** – odpowiadającą trybowi sterowania pozycją.

W kolejnym kroku zadajemy **prędkość ruchu** w parametrze **Profile Velocity (0x6081).** Wartości prędkości powinny zawierać się w zakresie od 0 do 3000 rpm [obroty/minutę].

Następnie zdefiniuj **przyspieszenie** dla ruchu w parametrze **Profile Acceleration (0x6083)**. Wartość tę wpisz jako czas w milisekundach, w którym zostanie zrealizowane przyspieszenie od spoczynku do prędkości znamionowej serwonapędu (rated speed).

Ustaw **ograniczenie momentu siły** dla serwonapędu **Max Torque (0x6072),** np. wartość 100 (przykładowo, wartość ok. 40 jest wartością progową dla pokonania oporów w samym silniku). Ta wartość podawana jest w dziesiątych częściach procenta, a więc wartości 1000 będzie odpowiadać 100% znamionowego momentu siły silnika.

Zadaj **pozycję dla ruchu** w parametrze **Target Position (0x607A).** Jednostki to: user unit. Przykładowo, wpisując wartości 100 000 spowodujesz wykonanie 10 pełnych obrotów (w przypadku użycia silnika z wbudowanym enkoderem 2500 działek/obrót, tj. 10 000 impulsów/obrót).

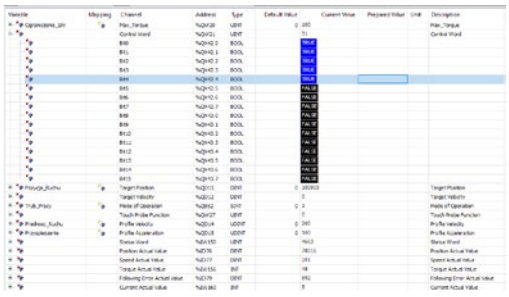
Ostatnim krokiem będzie przejście do **słowa kontrolnego Control Word (0x6040).** Rozwiń je i w celu załączenia serwonapędu załącz cztery najmniej znaczące bity tego słowa. Należy je zmienić na wartość **TRUE**, ponieważ przed załączeniem ruchu serwonapęd musi być w stanie gotowości. Zalecana kolejność załączania bitów to:

1. Enable Voltage
2. Quick Stop
3. Switch On
4. Enable Operation

Teraz możesz wydać polecenie ruchu, a więc załączyć dodatkowo bity 4, 5, 6 (co jest równe wartości 127 dziesiętnie). Odpowiada to załączeniu trzech kolejnych bitów: **New set-point**, **Change set immediately**, **Absolute/Relative**. Po załączeniu bitów kontrolnych oś serwonapędu jest sterowana zadaną wartością prędkości i momentu siły.

Zatrzymanie ruchu może odbyć się przez wyzerowanie zezwoleń na ruch w słowie kontrolnym **Control Word (0x6040)** albo przez załączenie ósmego bitu w tym słowie, tj. **bitu Halt**.

Tak powinna wyglądać nasza lista parametrów z przykładowymi wartościami podczas włączenia trybu RUN, gdy rzeczywiście nasz serwonapęd działa i możemy zaobserwować obrót serwosilnika.



Jeżeli serwonapęd zgłosił błąd (np. na skutek niewłaściwie zadanych parametrów ruchu – przykładowo błąd o kodzie Er22-0 w przypadku

nieutrzymania pozycji na skutek zadania zbyt małego momentu siły), można go skasować, zmieniając stan bitu kontrolnego **Fault Reset** z 0 na 1 w słowie kontrolnym, tj. bit 7 w Control Word (0x6040).

Praca w trybie sterowania prędkością

Teraz zobaczysz, w jaki sposób serwonapęd realizuje ruch z zadaną prędkością. Zmiany prędkości realizowane są zgodnie z zadanym przyspieszeniem.

Pierwszy krok jest analogiczny, jak w poprzednim trybie pracy. Zacznij od połączenia się ze sterownikiem.

Następnie ustawiamy tryb pracy – parametr **Mode of Operation (0x6060)** na wartość **3** – odpowiadającą trybowi sterowania prędkością.

Teraz zdefiniuj **przyspieszenie dla ruchu** w parametrze **Profile Acceleration (0x6083)**. Wartość tę wpisz jako czas w milisekundach, w którym zostanie zrealizowane przyspieszenie od spoczynku do prędkości znamionowej serwonapędu (rated speed).

Następnie w parametrze **Profile Deceleration (0x6084)** zadaj **przyspieszenie dla hamowania**. Wartość zadawana jest w milisekundach, jako czas hamowania od prędkości znamionowej serwonapędu do zatrzymania. Jeśli nie posiadasz tego parametru, dodaj go w następującym formacie: Data type: UDINT, Bit length: 32.

Przejdź do **słowa kontrolnego Control Word (0x6040).** Rozwiń je i w celu załączenia serwonapędu załącz cztery najmniej znaczące bity tego słowa. Należy je zmienić na wartość **TRUE**, ponieważ przed załączeniem ruchu serwonapęd musi być w stanie gotowości. Zalecana kolejność załączania bitów to:

1. Enable Voltage
2. Quick Stop
3. Switch On
4. Enable Operation

Następnie musimy **zadać prędkość ruchu** w parametrze **Target Velocity (0x60FF)**, w przeciwieństwie do trybu pozycjonowania nie jest to zmienna Profile Velocity (0x6081). Prędkość zadawana jest w obrotach na minutę. W odróżnieniu od procedury sterowania pozycją, w metodzie regulacji prędkości zmiana wartości zadanej prędkości spowoduje natychmiastową reakcję silnika serwonapędu.

Zmiana na ruchu parametrów, np. zadanej prędkości **Target Velocity (0x60FF)** oraz **momentu siły Max Torque (0x6072)**, zostanie natychmiast zrealizowana przez serwonapęd.

Tak powinna wyglądać nasza lista parametrów z przykładowymi wartościami podczas włączenia trybu RUN, gdy rzeczywiście nasz serwonapęd działa i możemy zaobserwować obrót serwosilnika, w trakcie pracy w trybie sterowania prędkością.

Variable	Mapping	Channel	Address	Type	Default Value	Current Value	Prepared Value	Unit	Description
Czas_hamowania		Profile deceleration	%QD10	UDINT	0	80			Profile deceleration
Ograniczenie_Sily		Max_Torque	%QW22	UINT	0	100			Max_Torque
		Control Word	%QW23	UINT		15			Control Word
		Bit0	%QX46.0	BOOL		TRUE			
		Bit1	%QX46.1	BOOL		TRUE			
		Bit2	%QX46.2	BOOL		TRUE			
		Bit3	%QX46.3	BOOL		TRUE			
		Bit4	%QX46.4	BOOL		FALSE			
		Bit5	%QX46.5	BOOL		FALSE			
		Bit6	%QX46.6	BOOL		FALSE			
		Bit7	%QX46.7	BOOL		FALSE			
		Bit8	%QX47.0	BOOL		FALSE			
		Bit9	%QX47.1	BOOL		FALSE			
		Bit10	%QX47.2	BOOL		FALSE			
		Bit11	%QX47.3	BOOL		FALSE			
		Bit12	%QX47.4	BOOL		FALSE			
		Bit13	%QX47.5	BOOL		FALSE			
		Bit14	%QX47.6	BOOL		FALSE			
		Bit15	%QX47.7	BOOL		FALSE			
Pozycja_Ruchu		Target Position	%QD12	DINT	0	0			Target Position
Predkosc_Ruchu_PREDKOSC		Target Velocity	%QD13	DINT	0	200			Target Velocity
Tryb_Pracy		Mode of Operation	%QB56	SINT	0	3			Mode of Operation
		Touch Probe Function	%QW29	UINT		0			Touch Probe Function
Predkosc_Ruchu_POZYCJA		Profile Velocity	%QD15	UDINT	0	0			Profile Velocity
Przyspieszenie		Profile Acceleration	%QD16	UDINT	0	100			Profile Acceleration
		Status Word	%IW150	UINT		1591			Status Word
		Position Actual Value	%ID76	DINT		102286			Position Actual Value
		Speed Actual Value	%ID77	DINT		201			Speed Actual Value
		Torque Actual Value	%IW156	INT		41			Torque Actual Value
		Following Error Actual Value	%ID79	DINT		0			Following Error Actual Value
		Current Actual Value	%IW160	INT		4			Current Actual Value

Świetnie! Dzięki pierwszej części tego odcinka zrozumiałeś istotę działania danego trybu pracy zainicjowanego komunikacją EtherCAT. W drugiej części pokażę Ci, w jaki sposób za pomocą języka LD oraz wprowadzenia wizualizacji HMI możesz stworzyć swoją własną aplikację. •

↳ Drugą część znajdziesz na Poradniku Automatyka: www.astor.com.pl/poradnikautomatyka/komunikacja-ethercat-konfiguracja-i-przykladowa-aplikacja-w-srodowisku-codesys-czesc-2-kurs-obslugi-i-konfiguracji-serwonapedow-astraada-srv-odc-3/

Kompletny kurs obsługi i konfiguracji serwonapędów Astraada SRV znajdziesz na stronie Poradnika Automatyka:

↳ www.astor.com.pl/poradnikautomatyka/kurs-obslugi-i-konfiguracji-serwonapedow-astraada-srv/

Jak przeprowadzić serwis robota przemysłowego?

Automatyzacja w przemyśle to nie tylko trend, lecz przede wszystkim klucz do osiągnięcia wyższej efektywności i konkurencyjności. Ważnym aspektem w dziedzinie robotyki i automatyki jest serwis.

» Przyjrzyjmy się zatem, jakie kluczowe kroki są podejmowane w firmie Tauron Wydobycie, by zagwarantować nie tylko sprawną pracę robotów, lecz także osiągnięcie optymalnych wyników w dziedzinie produkcji przemysłowej.

Pod lupę bierzemy etapy serwisu robota przemysłowego Kawasaki Robotics w firmie Tauron Wydobycie, służącego do układania na paletę worków z węglem.

Przedstawiamy 13 etapów serwisu robota:

Etap 1. Przygotowanie do serwisu
Serwisant ubiera się w odpowiedni strój ochronny, a także przygotowuje niezbędne narzędzia i części zamienne.

Etap 2. Bezpieczeństwo na miejscu pracy
Zanim przystąpi się do prac serwisowych, konieczne jest zabezpieczenie otoczenia. Miejsce pracy jest wygrodzone barierami ochronnymi lub taśmami, gwarantując bezpieczeństwo pracowników.

Etap 3. Zgranie backupu z robota i dokumentacja znamionowa
Zgrywamy backup z robota oraz robimy zdjęcia parametrom robota w celu zachowania porządku w bazie danych oraz wygenerowania raportu po wizycie.

Etap 4. Pozycjonowanie robota
Robot jest przestawiany w wygodną pozycję do dalszych prac oraz tak, aby nie zagrażał nikomu w razie niekontrolowanej awarii.

Etap 5. Montaż belki usztywniającej
Aby uniknąć kolizji i zapewnić stabilność ramion robota, montowana jest belka usztywniająca.

Etap 6. Demontaż sprężyn gazowych
Odkręcamy śruby i wyjmujemy sprężyny.

Zamontowana belka usztywniająca na robocie. Źródło: Tauron Wydobycie

Etap 7. Wymiana na nowe sprężyny
W miejsce starych montujemy nowe sprężyny.

Etap 8. Sprawdzanie poziomu ciśnienia w sprężynach
Optymalna wartość powinna mieścić się między 8.0, a 9.0 MPa.

Robot Kawasaki Robotics CP180L-AC02. Źródło: Tauron Wydobycie

Etap 9. Wymiana serwonapędu
Wymieniamy serwonapęd odpowiedzialny za ruchy robota. Serwonapęd pełni kluczową rolę w uruchomieniu ruchu zarówno całego zespołu przekładni, jak i poszczególnych osi robota.

Etap 10. Przekładnia wałka
Wymagany wałek zostaje przeniesiony ze starego serwa.

Etap 11. Kalibracja trzech osi
Przeprowadzona zostaje kalibracja trzeciej osi, aby uzyskać precyzję i dokładne ruchy robota.

Etap 12. Testy i sprawdzenie
Robot przechodzi serię testów, aby upewnić się, że działa prawidłowo i zgodnie z oczekiwaniami.

Etap 13. Sporządzenie raportu
Cały proces dokładnie dokumentujemy w raporcie. •

AUTOR: **Adrian Kociarz**

→ Coboty – współpraca człowieka z robotem, jakiej jeszcze nie było

Cobot, inaczej robot współpracujący, to kolejny krok w rozwoju robotyzacji przemysłu. Radosław Kołacz, starszy specjalista ds. robotów przemysłowych w firmie ASTOR, w wywiadzie opowiada o tym, gdzie najlepiej zastosować coboty oraz jak zapewnić bezpieczną pracę człowieka z cobotem.

Katarzyna Szkopek: Czym tak właściwie jest cobot?

Radosław Kołacz: W zasadzie jeszcze nie ma jasnej definicji dla robota współpracującego, zatwierdzonej przez ISO (Międzynarodową Organizację Normalizacyjną). Aktualnie jest tylko definicja dla operacji współpracującej. A jest to stan, w którym specjalnie zaprojektowany robot pracuje w bezpośrednim towarzystwie z człowiekiem w określonej przestrzeni roboczej. Znaczy to, że człowiek i robot mogą pracować blisko siebie, nie muszą być w żaden sposób od siebie oddzieleni, a co więcej, kontakt między robotem a operatorem może mieć miejsce, jeśli są zachowane odpowiednie środki bezpieczeństwa.

Jakie są cechy charakterystyczne cobota?

Radosław Kołacz: Najważniejszą cechą współpracujących robotów jest ich zdolność do współdziałania z ludźmi, jednocześnie nie stanowiąc zagrożenia dla bezpieczeństwa pracowników. Coboty nie wymagają zewnętrznego systemu bezpieczeństwa – ludzie mogą swobodnie poruszać się w ich otoczeniu, a wbudowany system detekcji kolizji pozwala robotowi zatrzymać się automatycznie w przypadku wykrycia kontaktu z drugim obiektem lub osobą.

Inną charakterystyczną cechą współpracy jest możliwość manualnego sterowania, umożliwiająca człowiekowi precyzyjne przemieszczenie ramienia robota oraz przesunięcie go w określone miejsce.

Aby zagwarantować bezpieczeństwo, coboty są projektowane w szczególny sposób, ograniczając ich siłę i prędkość. Dzięki temu nie są w stanie osiągnąć zbyt dużych prędkości lub wywierać dużego nacisku na obiekty, z którymi wchodzą w interakcję. Jeśli parametry te zostaną przekroczone, robot automatycznie zatrzyma się, aby chronić pracowników.

Kolejnym aspektem zapewniającym bezpieczeństwo jest wbudowany mechanizm chroniący przed przypadkowym przytrzaśnięciem. Coboty mają niewielkie podstawy, co pozwala na ich zamontowanie na stanowiskach produkcyjnych o ograniczonej powierzchni.

Programowanie robotów nie jest szczególnie trudne, zamiast tradycyjnego kodowania używa się interaktywnych bloczków, co znacząco skraca czas nauki programowania, nawet dla osób bez wcześniejszego doświadczenia w obszarze robotyki.

Jaka jest różnica między robotem przemysłowym a cobotem?

Radosław Kołacz: Roboty przemysłowe charakteryzują się dużymi prędkościami oraz udźwigiem od kilku kg do ponad tony, bardzo dużą wydajnością i powtarzalnością. Z kolei wybierając coboty ▷

zyskujemy bezpieczeństwo bliskiej współpracy na stanowisku, możemy również łatwiej obsługiwać i programować robota współpracującego.

Kiedy lepiej zastosować cobota, a kiedy robota przemysłowego?

Radosław Kołacz: Dzięki łatwości przezbrojenia i elastyczności wdrożenia coboty mogą być używane do obsługi prostych aplikacji oraz takich, gdzie robot często jest przenoszony w inne miejsce lub przezbrajany do innego zadania, np. przy produkcji małoseryjnej. Z kolei jeżeli operacja jest bardzo powtarzalna i wymaga wysokiej wydajności, to lepiej sprawdzi się robot przemysłowy.

W większości przypadków cena robota współpracującego jest wyższa niż jego przemysłowego odpowiednika, jednak w przypadku cobotów nie ma konieczności montażu wygrodzeń czy podpinania systemu safety, tak jak ma to miejsce w przypadku wdrażania robota przemysłowego. Dzięki temu jeżeli przestrzeń na wdrożenie robota jest ograniczona i nie chcemy budować dużej klatki otaczającej stanowisko, to w takiej aplikacji lepiej sprawdzi się cobot.

Minusem cobotów jest to, że nie można realizować z nimi bardziej zaawansowanych aplikacji, więc jeżeli potrzebujemy aby robot wykonywał skomplikowaną logikę, to lepiej sprawdzi się robot przemysłowy.

Coboty nie są szybkimi robotami i stosuje się je tam, gdzie nie zależy nam na pełnej wydajności czy powtarzalności, a jedynie na aplikacji, w której człowiek może współpracować z robotem. Dodatkowo udźwig cobotów w ofercie Kawasaki Robotics jest ograniczony, największy to 10 kilogramów, co może wykluczyć pewne zastosowania. Tak więc robot przemysłowy będzie lepszym wyborem, jeżeli potrzebujemy większego udźwigu oraz jeżeli robot ma wykonywać dużo różnych czynności jednocześnie – większe skomplikowanie narzędzia robota powoduje wzrost jego wagi i zmniejszenie bezpieczeństwa jego użytkowania, a tym samym konieczność odseparowania przestrzeni pracy robota od przestrzeni, w której pracują ludzie.

W jakich branżach na rynku i firmach mogą być wykorzystane coboty?

Radosław Kołacz: Warto je stosować przy obsłudze maszyn CNC – robot może pobierać detale, a następnie umieszczać je w maszynie, dzięki czemu operator może w tym czasie realizować inne zadania.

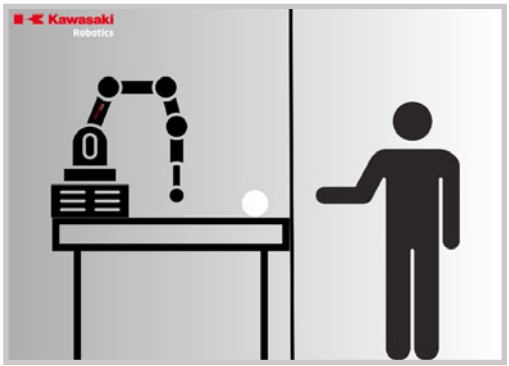
Co warto podkreślić, coboty dobrze sprawdzają się we wszystkich powtarzalnych operacjach jak np. paletyzacja, szlifowanie czy malowanie. Łatwiej określić sytuacje, w których nie powinno się ich używać, a do nich należą strefy zagrożone wybuchem. Warto wykorzystać coboty w branży elektronicznej – przekładanie i umieszczanie komponentów SMD (elementy elektroniczne przeznaczone do montażu powierzchniowego), technologie PTH, czy w operacjach montażu, gdzie człowiek współpracuje z robotem, który przekłada elementy podane przez pracownika.

Jak wygląda współpraca cobota z człowiekiem?

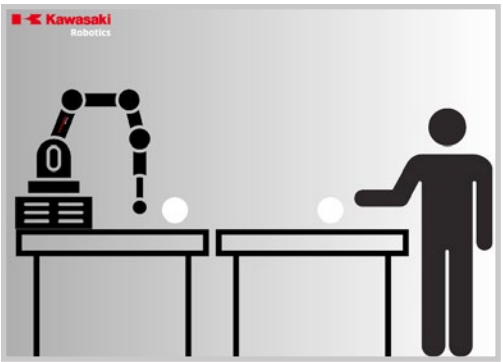
Radosław Kołacz: Współpraca cobota z człowiekiem znacząco różni się od współpracy ze standardowym robotem przemysłowym. Zadania mogą być wykonywane w tym samym czasie na jednej przestrzeni. Nie ma zagrożenia, że dojdzie do wypadku, ponieważ cobot momentalnie przerywa pracę w momencie kontaktu z obcym obiektem lub człowiekiem.

Możemy wyróżnić kilka poziomów aplikacji współpracujących między robotami a człowiekiem:

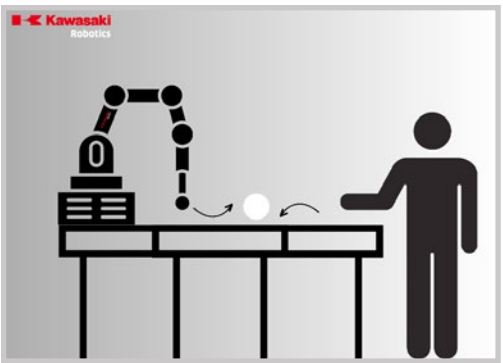
Pierwszą z nich to **stanowisko**, gdzie człowiek nie ma dostępu do miejsca, w którym pracuje cobot, ponieważ jego stanowisko jest odgrodzone od pracownika.



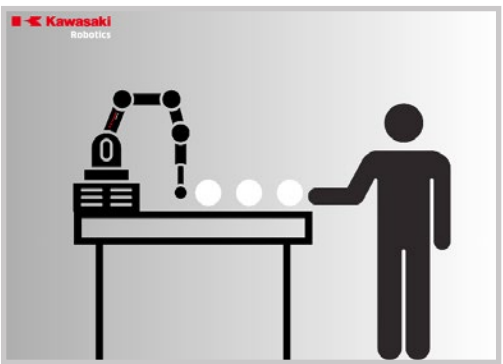
Następnym poziomem jest **koegzystencja**, w której raz na jakiś czas człowiek dostarcza robotowi detale, ale ich interakcje są okazjonalne.



W **synchronizacji** człowiek i cobot dzielą przestrzeń roboczą, ale nie w tym samym czasie.



W ramach **współdziałania** dzielą w tym samym czasie przestrzeń roboczą, ale wykonują inne czynności.



Współpracując, cobot i człowiek dzielą detale, jak i przestrzeń, pracując w tym samym czasie.

Podsumowując, tam gdzie robot i człowiek dzielą przestrzeń, ze względów bezpieczeństwa najlepszym rozwiązaniem jest cobot. Dlatego dzięki wprowadzeniu cobotów możemy je traktować jak kolejnego pracownika.

Jakie są zastosowania cobotów?

Radosław Kołacz: Głównymi aplikacjami, w których warto korzystać z cobotów, są: paletyzacja, spawanie, montaż, malowanie czy obsługa maszyn CNC, w tym szeroko pojęty handling. Co ciekawe, mimo, że może się wydawać, że do malowania bardziej sprawdziłyby się standardowe roboty przemysłowe, to na rynku coraz większą popularnością cieszą się coboty odpowiednio dostosowane do malowania. Szczególnie zachęcający jest fakt, że obsługa cobota jest ułatwiona ze względu na możliwość wodzenia za kiść i ręcznego dostosowywania pozycji ramienia.

Kiedy i gdzie można zobaczyć cobota?

Radosław Kołacz: Cobot jest już dostępny do obejrzenia w ASTOR Robotics Center, możemy go także zaprezentować bezpośrednio u klienta.

Jaka jest rola firmy ASTOR jako dystrybutora i jakie jest wsparcie techniczne cobotów?

Radosław Kołacz: W ASTOR zawsze mówimy, że jesteśmy dostawcą technologii i wiedzy, i w tym przypadku nie jest inaczej. Widząc ogromne zainteresowanie cobotami na polskim rynku, postanowiliśmy dołączyć je do naszej oferty.

Dziękujemy za rozmowę. •

ROZMAWIAŁA: **Katarzyna Szkopek**
Dział Rozwoju Sprzedaży i Marketingu Robotyki, ASTOR

Informacje dodatkowe dotyczące ulgi na robotyzację w kontekście cobotów:

Ulga na robotyzację obowiązuje od 1 stycznia 2022 do 31 grudnia 2026 roku i obejmuje koszty powiązane z robotyzacją poniesione przez przedsiębiorców (poza działalnością rolniczą). Na ulgę można wpisać roboty przemysłowe, osprzęt i peryferia, urządzenia takie jak tory jezdne, pozycjonery, czujniki, ale i szkolenia.

A jakie warunki należy spełnić, żeby uzyskać częściowy zwrot kosztów? Po pierwsze trzeba sobie odpowiedzieć na pytanie, czym jest robot, a zgodnie z definicją zawartą w ustawie jest to: „urządzenie techniczne przemysłowe, zastosowane w przemyśle, które ma służyć produkcji. Jest maszyną o 3 stopniach swobody (z co najmniej 3-osiami) lub robotem mobilnym, z możliwością podłączenia do sieci przemysłowej i przekazywania danych produkcyjnych. Musi być także swobodnie programowalny oraz fabrycznie nowy".

KONTAKT WS. COBOTÓW:
Radosław Kołacz
Starszy specjalista ds. robotów przemysłowych
radoslaw.kolacz@astor.com.pl
www.astor.com.pl

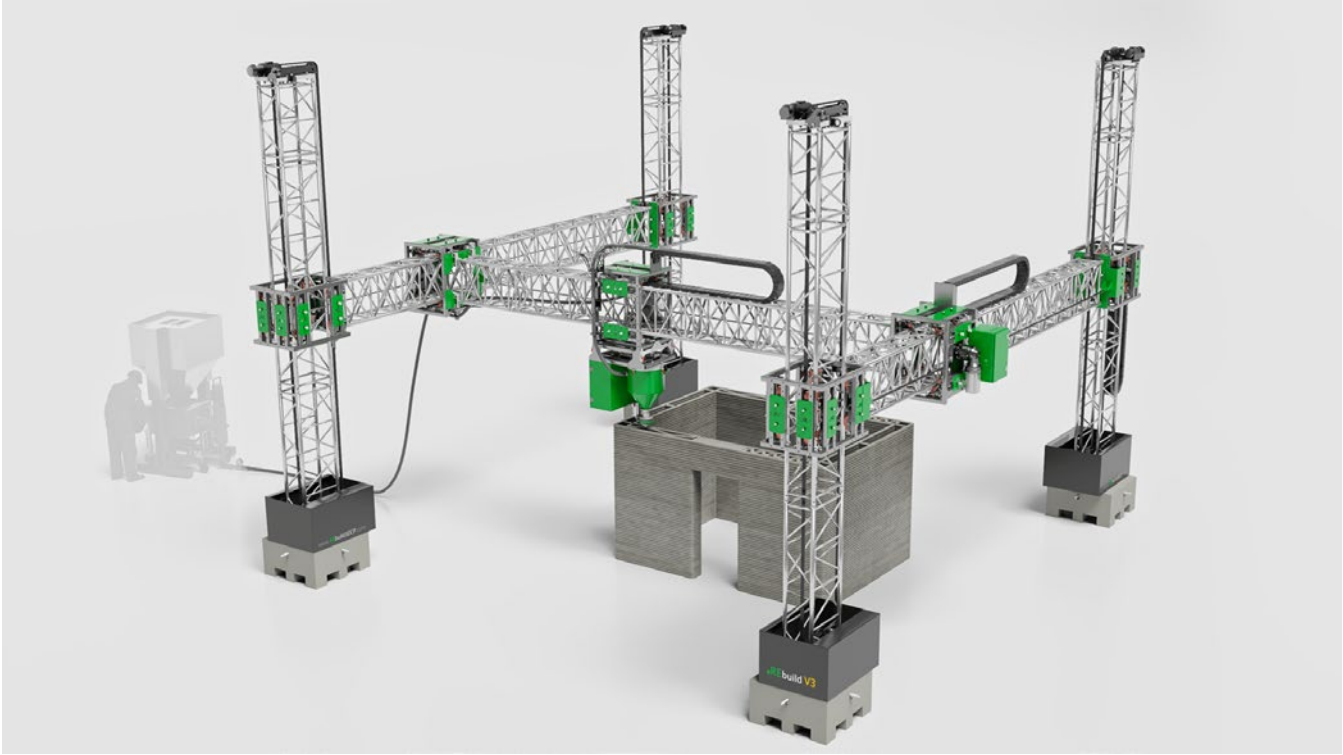
Sterownik Astraada One w wielkogabarytowej drukarce 3D do zadań konstrukcyjnych

Od lat 80-tych XX wieku obserwujemy dynamiczny rozwój technologii wytwarzania addytywnego. Większość z tych rozwiązań wykorzystywana jest do prototypowania i tworzenia niewielkich detali w szerokim spektrum branż, takich jak medycyna, motoryzacja czy przemysł spożywczy. Może to zredukować czasochłonne i kosztowne etapy produkcji wszędzie tam, gdzie mamy do czynienia ze złożonymi geometriami.

Przykład realizacji budynku. Źródło: https://www.rebuild3dcp.com/

» Można jednak zadać pytanie: co może się stać, gdy zastosujemy takie rozwiązanie do celów konstrukcyjnych w wielkogabarytowej drukarce 3D, integrując wszystkie serwomotory z najnowszymi urządzeniami z rodziny Astraada One? Odpowiedzi udzielił zespół inżynierów z REbuild, wspierany przez ekspertów firmy ASTOR.

REbuild to firma zatrudniająca doświadczonych ekspertów – inżynierów, którzy chcą zrekonstruować sposób budowania. Jest to niedawno założony startup zajmujący się wprowadzaniem druku 3D do branży budowlanej. Zespół REbuild wypracował rozwiązania technologiczne dla branży budowlanej, takie jak techniki zbrojeń, szalunków, podpór, izolacji termicznej czy skomplikowanych kształtów ścian, koncentrując się na automatyzacji procesów



Wizualizacja drukarki 3D, źródło: https://www.rebuild3dcp.com/

wytwarzania tego typu elementów. Ponadto firma posiada know-how w zakresie technologii recyklingu, umożliwiającej ponowne wykorzystanie surowców w procesie budowy. Oferowane przez REbuild rozwiązania skracają czas i koszty budowy o połowę.

Firma ASTOR chętnie wspiera rozwój zarówno projektów OEM, jak i R&D. W tym przypadku głównym celem była integracja 16 serwomotorów z niestandardowym systemem nadrzędnym i urządzeniami bezpieczeństwa. REbuild poszukiwał elastycznego rozwiązania, wykorzystującego otwarty standard programowania CODESYS, obsługującego szeroką gamę protokołów komunikacyjnych, charakteryzującego się łatwym w użyciu interfejsem, a przede wszystkim sprawdzonego i przetestowanego w maszynach CNC.

Sercem systemu jest najnowszy modułowy sterownik PLC Astraada One Modular Pi-Prime oraz moduł bezpieczeństwa Astraada One Modular SAFETY SC-1000 dla bezpieczeństwa maszyn. Zastosowanie sterownika PLC z protokołem komunikacyjnym EtherCAT pomaga osiągnąć szybki czas reakcji i precyzyjną kontrolę pozycjonowania.

Możliwość zaprogramowania zarówno sterowników PLC, jak i sterowników bezpieczeństwa w jednym otwartym środowisku CODESYS jest dużym ułatwieniem dla inżynierów automatyki i pomaga skrócić czas wdrożenia. Dodatkowo zastosowane rozwiązanie w postaci sterownika Astraada One Modular Pi-Prime oparte jest na platformie Raspberry Pi, która zapewnia dużą wydajność przy zachowaniu kompaktowych wymiarów, dzięki czemu sprawdza się doskonale jako element składowy rozwijanego przez REBuild nadrzędnego systemu sterowania.

Dzięki owocnej współpracy i wymianie doświadczeń ekspertów ASTOR i REbuild w zakresie sterowania liniowego jesteśmy świadkami bardzo ważnej innowacji w branży inżynierii lądowej i produkcji addytywnej. Firma REbuild z pewnością nie osiądzie na laurach, dlatego czekamy z niecierpliwością na kolejne innowacyjne projekty. •

Przykład wydruku EDCP. Źródło: https://www.rebuild3dcp.com/

Sterownik PLC Astraada One Modular Pi-Prime. Źródło: ASTOR

Moduł bezpieczeństwa Astraada One Modular SAFETY SC-1000. Źródło: ASTOR

Sercem systemu jest najnowszy modułowy sterownik PLC Astraada One Modular Pi-Prime oraz moduł bezpieczeństwa Astraada One Modular SAFETY SC-1000 dla bezpieczeństwa maszyn. Zastosowanie sterownika PLC z protokołem komunikacyjnym EtherCAT pomaga osiągnąć szybki czas reakcji i precyzyjną kontrolę pozycjonowania.

Kurnik KROPPER model Eko 100. Źródło: KROPPER

Panele Astraada HMI w mobilnych kurnikach KROPPER

Panele operatorskie to jedne z najczęściej spotykanych urządzeń automatyki w przemyśle. Znajdziemy je na liniach produkcyjnych, w maszynach, przy stanowiskach zrobotyzowanych. Ich zastosowania nie ograniczają się jednak tylko do zakładów produkcyjnych. Panele Astraada HMI możemy znaleźć także w mobilnych kurnikach.

» Firma KROPPER została założona w 2021 roku przez Patryka i Aleksandrę Mrowińskich. W ciągu dwóch lat stała się czołowym producentem mobilnych kurników w Polsce. Swoje produkty sprzedaje w całej Europie, przede wszystkim w Niemczech, Austrii, Belgii, a także w Szwajcarii i Czechach. Produkowane przez KROPPER kurniki zostały zaprojektowane przez Patryka Mrowińskiego, we współpracy z doświadczonymi konstruktorami.

Czym jest mobilny kurnik?

Kurniki mobilne są nowoczesną i ekologiczną formą tradycyjnego kurnika. Z wyglądu przypominają pojazd lub przyczepę i umożliwiają łatwe przemieszczanie hodowli zarówno na obszarze własnego gospodarstwa, jak i poza nim. Przeznaczone są do wolnowybiegowego chowu kur, przy czym hodowla spełnia wszystkie normy narzucane przez przepisy prawa. Konstrukcja kurnika umożliwia przemieszczanie stada w inne miejsce, co wpływa na urozmaicenie pożywienia kur, a także daje możliwość odnowienia pastwiska.

W ofercie KROPPER znajdziemy modele, w których można hodować 225 kur w chowie ekologicznym lub 340 w chowie wolnowybiegowym, a także mniejsze rozwiązania, dla 106 kur hodowanych ekologicznie lub 160 na wolnym wybiegu. Kurniki są bardzo starannie zaprojektowane i nie ma w nich elementów przypadkowych. W procesie produkcyjnym wykorzystano najnowocześniejsze rozwiązania z zakresu obróbki metali. Do budowy kurnika wykorzystywane są elementy ze stali nierdzewnej, a cała konstrukcja stalowa jest cynkowana ogniowo, co stanowi niezawodne zabezpieczenie przed korozją.

Co w środku?

Każdy kurnik składa się z kilku podstawowych elementów funkcjonalnych, przy czym konstrukcja jest bardzo elastyczna. Dzięki temu możliwe jest dostosowanie gotowego produktu do indywidualnych potrzeb klienta.

Najważniejszymi elementami kurnika są: grzędy, systemy podawania paszy i wody, gniazda (w których kury składają jaja), wrota wyjściowe (poprzez które kury mogą opuszczać kurnik i powracać do niego), wentylatory, panele solarne (zamontowane na dachu), wspomagane dodatkowymi akumulatorami, a także specjalny system umożliwiający czyszczenie wnętrza kurnika. Całość nadzoruje system automatyki, który steruje większością z tych elementów (w prostszych modelach niektóre z nich mogą być obsługiwane ręcznie).

Kurnik KROPPER model Eko 225. Źródło: KROPPER

Automatyka przemysłowa w mobilnym kurniku

System automatyki w kurnikach KROPPER wykorzystuje **panel operatorski Astraada HMI**, który współpracuje z prostym sterownikiem PLC Siemens Logo. Całość pracuje w trybie automatycznym, choć oczywiście jest możliwość przełączenia się w tryb ręczny, w celach testowych lub serwisowych.

System steruje oświetleniem w kurniku, zarówno górnym, jak i specjalnym oświetleniem dolnym, które wykorzystywane jest, aby „zachęcić" kury do wieczornego powrotu do kurnika. Godziny włączenia i wyłączenia oświetlenia ustawiane są przez operatora, a dodatkowo możemy zainstalować czujnik zmierzchu, który pozwala sterować lampami w zależności od jasności na zewnątrz.

Drugim elementem sterowanym przez automatykę są wrota prowadzące na wybieg – operator programuje godzinę ich otwarcia i zamknięcia. Podobnie sterowane są wewnętrzne klapy zapewniające dostęp do gniazd, przy czym tu automatyzacja zależna jest od wersji kurnika. Otwieranie może być całkowicie zautomatyzowane (otwarcie i zamknięcie o danej godzinie), lub też automatyczne może być tylko otwarcie – wtedy gniazda zamykane są ręcznie przed wyjęciem jaj przez obsługę.

W modelu Auto-Feeder 225 w trybie automatycznym sterowane są również paśniki – system zarządza uzupełnianiem poziomu paszy, a także pozwala monitorować jej poziom w zbiorniku. Dodatkowo automatycznie sterowane są również wentylatory i okna (które mogą być otwierane w razie

> *„Panele Astraada HMI są idealnym dopełnieniem zamysłu, który mieliśmy podczas tworzenia naszych kurników. Dzięki panelom obsługa kurników jest bardzo prosta i intuicyjna. Ponadto zespół ASTOR pomógł nam wdrożyć niedostępne do tej pory funkcjonalności, takie jak zdalna obsługa kurnika. Wpłynęło to na wzrost konkurencyjności naszych produktów oraz na atrakcyjność naszej oferty".*
>
> – Patryk Mrowiński, KROPPER

Szafa sterownicza w kurniku. Źródło: KROPPER

Panel Astraada HMI z uruchomioną aplikacją. Źródło: ASTOR

Zdalny dostęp do panelu HMI za pośrednictwem IDCS. Źródło: KROPPER

potrzeby) – ma to na celu zapewnienie właściwej temperatury w kurniku.

Panel operatorski Astraada HMI umożliwia z jednej strony wprowadzanie wszystkich ustawień, a z drugiej – pozwala monitorować wszystkie kluczowe parametry. Z poziomu aplikacji HMI operator wprowadza nastawy dla pracy automatycznej, ale może też ręcznie sterować poszczególnymi elementami kurnika.

Zdalny dostęp do aplikacji wizualizacyjnej

Bardzo cenną funkcjonalnością, udostępnianą przez panele operatorskie Astraada HMI, jest **możliwość zdalnego dostępu do aplikacji**. Jest to możliwe dzięki standardowi IDCS, który jest obsługiwany przez wszystkie panele Astraada. IDCS zapewnia pełen dostęp do aplikacji uruchomionej na panelu za pośrednictwem Internetu. Innymi słowy – operator ma dostęp do aplikacji z dowolnego urządzenia wyposażonego w przeglądarkę internetową: komputera, tabletu lub smartfonu.

Stanowi to niebagatelne ułatwienie dla pracowników zajmujących się obsługą kurnika, który przecież zwykle stoi na pastwisku, nieraz dość odległym. Dzięki IDCS nie muszą oni być na miejscu, aby mieć dostęp do aplikacji wizualizacyjnej. Na ekranie swojego smartfona **mogą widzieć dokładnie to samo, co na panelu**, i mogą też dokładnie to samo zrobić (np. zmienić ustawienia). Dzięki zdalnemu dostępowi można też monitorować wszystkie ważne parametry, jak np. temperaturę, poziom paszy czy poziom wody.

Podsumowanie

Firma KROPPER udowodniła, że w Polsce mogą powstawać nowatorskie i bardzo konkurencyjne rozwiązania technologiczne, które wzbudzają duże zainteresowanie w całej Europie.

Przykład mobilnych kurników pokazuje, że zastosowania typowych urządzeń automatyki, takich jak panele operatorskie Astraada HMI, nie muszą ograniczać się wyłącznie do obszaru produkcji przemysłowej. •

AUTOR:
Mateusz Pierzchała

KROPPER Patryk Mrowiński
Dębicze 56
63-520 Grabów nad Prosną
www.mobilekropper.com

ASTOR

ZAKUPY 24H/7 | ATRAKCYJNE PROMOCJE | SZEROKA OFERTA PRODUKTÓW | WSPARCIE TECHNICZNE ASTOR

NOWOŚCI I PROMOCJE W SKLEPIE INTERNETOWYM FIRMY ASTOR

www.astor.com.pl/sklep

→ Zestaw startowy - PACSystems RSTi-EP CPE205 + 32DI + 32 DO

Kod produktu: EPXCPE205SET-PR
Producent: Emerson

5260 PLN NETTO

Jednostka centralna z wbudowanym modułem komunikacyjnym i zasilaczem systemowym.

Zestaw zawiera:

- 1× EPXCPE205 – PACSystems RSTi-EP CPE205; 0.5MB RAM i FLASH; 1.2 GHz Dual Core; 2× Eth; 1× RS232; 2× USB
- 2× EP-125F – 16 wejść dyskretnych 24VDC; logika dodatnia; diagnostyka
- 2× EP-225F – 16 wyjść dyskretnych 24VDC; 0.5A; logika dodatnia

→ Sterownik PLC z terminalem HMI Astraada One Compact HMI DC2110W X CS

Kod produktu: S-01010104-0405-PR
Producent: Astraada

6700 PLN NETTO

~~8080~~ PLN
–17%

- wysokiej jakości ekran pojemnościowy 10,1" (1280 × 800 pikseli), MultiTouch
- 4 wejścia dyskretne, 4 wyjścia dyskretne, 4 wejścia analogowe
- porty komunikacyjne Ethernet, CAN, RS232/RS485, USB
- EtherCAT, CAN, CANOpen, Modbus TCP/IP, Modbus RTU
- obsługa SoftMotion/SoftMotion+CNC

→ Switch zarządzalny przemysłowy, Ethernet – 10-portowy – promocja

Kod produktu: JET-NET-5010G-W
Producent: Astraada

2690 PLN NETTO

~~3020~~ PLN
–11%

- 7 portów 10 / 100-TX oraz 3 porty combo RJ-45/SFP (10/100/1000 Base-TX, 100 Base-FX, 1000 Base-FX)
- redundancja: RSTP, Rapid Super Ring (czas przywracania <5ms),Rapid Dual Homing
- solidna aluminiowa obudowa o stopniu ochrony IP31
- temperatura pracy -40...70°C
- 54 miesiące gwarancji

→ Zestaw szkoleniowy Astraada HMI – dotykowy panel 7", zasilacz, szkolenie online, oprogramowanie i podręczniki

Kod produktu: AS45TFT0703-SZK
Producent: Astraada

1120 PLN NETTO

~~1750~~ PLN
–36%

Panel obsługuje ponad 400 driverów do komunikacji z większością urządzeń automatyki.

- Dotykowy panel operatorski o przekątnej 7" (matryca TFT COM1 – RS232, COM2 – RS422/485, COM3 – RS485, 2× USB (Client, Host), Ethernet, 64 MB RAM, 64 MB ROM, 128KB pamięci podtrzymywanej bateryjnie
- Przemysłowy zasilacz impulsowy 30W (24V/1.25A DC)
- Szkolenie online w postaci filmów instruktażowych
- Oprogramowanie narzędziowe (bezpłatne do pobrania)
- Zestaw dokumentacji

→ Robot edukacyjny ASTORINO

Kod produktu: ASTORINO-BASIC-B002
Producent: ASTOR

26500 PLN NETTO

Robot edukacyjny Astorino do nauki programowania, oparty o druk 3D, w wersji podstawowej, złożony.

- Robot edukacyjny o 6 stopniach swobody (jak robot przemysłowy)
- Kompletny system sterowania
- USB/Ethernet,
- Zasilacz 24V
- Oprogramowanie i komplet dokumentacji

→ Zestaw IPC + SCADA: komputer Astraada PC 21,5" Standard z licencją AVEVA Edge 2020

Kod produktu: AS54EDG1500-PR
Producent: Astraada, AVEVA

~~11830~~ PLN
−28%

8550 PLN NETTO

- Oprogramowanie wizualizacyjne AVEVA Edge 2020 Embedded HMI Runtime 1500
- Komputer AS54F22C462:
  - dotykowy ekran pojemnościowy LCD o przekątnej 21,5"
  - rozdzielczość: 1920 × 1080 px
  - procesor Intel Celeron J1900
  - 4 GB RAM
  - dysk SSD 128 GB
  - stopień ochrony IP65
  - system operacyjny Windows 10 IoT

→ Zestaw zdalnego dostępu do sterownika – router + sterownik PLC+HMI

Kod produktu: HEXT251C112-RUT955
Producent: Horner, Teltonika

~~7200~~ PLN
−53%

3390 PLN NETTO

- sterownik Horner PLC+HMI HEXT251C112
  - 12 DI
  - 6 DO (przekaźnikowe),
  - 4AI (0-20mA, 4-20mA, 0-10V)
  - ekran dotykowy, 3.5" TFT, 32k kolorów
  - zasilanie 9-30VDC
- router Teltonika RUT955
  - obsługa sieci 2G/3G/4G
  - 2 × sloty dla kart SIM (MINI SIM – 2FF), 1.8 V/ 3 V
  - 4 porty Ethernet 10/100 Mbps na złączach RJ45
  - zasilanie 9-30VDC
- dedykowany kurs
- gwarancja 24 miesiące

→ Zestaw startowy Astraada One Modular – Sterownik modułowy Pi-Pro + Moduł 16DI/16DO + Zasilacz 24 VDC + Targety + e-szkolenie

Kod produktu: ONE-START-MODULAR
Producent: Astraada

~~5700~~ PLN
−32%

3900 PLN NETTO

- Jednostka centralna MC Pi-Pro, wsparcie Codesys V3.5, 1.5 GHz QuadCore, 8GB Flash, 1GB RAM,1 × Ethernet, 1 × EtherCAT, 2 × USB 3.0, 1 × DDI
- Moduł wejść/wyjść cyfrowych: 16DI, 16DO (1 ms/0,5A), zasilacz impulsowy (110-220VAC / 24V/5A DC)
- Targety sterownika Astraada One dla oprogramowania CODESYS
- Szkolenie internetowe – Sterowniki PLC Astraada One – podstawy tworzenia aplikacji sterujących i wizualizacji

Regulamin promocji:

- Produkty w promocyjnych cenach dostępne są tylko w sklepie internetowym ASTOR
- Promocja obowiązuje do 31.12.2023 lub do wyczerpania stanów magazynowych
- Podane ceny są cenami netto w PLN

© Copyright: ASTOR Sp. z o.o. Wszystkie prawa zastrzeżone

→ Ludzie ASTORa (104)

Kamila Jaworowska

Młodszy inżynier ds. sprzedaży

Hejka! ☺

W kwietniu 2021 roku, jako stażystka, miałam przyjemność dołączyć do zespołu ASTOR, działającego na obszarze zachodnim. Moje pierwsze kontakty z firmą sięgają jednak nieco wcześniejszego czasu, kiedy to zostałam ambasadorką ASTOR na Politechnice Poznańskiej. Studiując automatykę i robotykę, w okresie pandemii, kiedy zajęcia praktyczne na uczelni stały się niemożliwe, poszukiwałam firmy, która pozwoliłaby mi rozwijać się już w „rzeczywistej" branży, z którą planowałam związać swoją przyszłość. Początkowo zakładałam, że będzie to krótka przygoda, trwająca może trzy miesiące, po czym przesiądę się do firmy zajmującej się programowaniem sterowników PLC. Jednakże sztuka łączenia umiejętności technicznych z kompetencjami miękkimi, kontakt z klientem i praca w zgranym, wspierającym się zespole tak bardzo przypadły mi do gustu, że zmieniłam swoje plany i postanowiłam kontynuować poszerzanie swojego doświadczenia w dziale sprzedaży, zamiast programowania sterowników.

Po okresie stażu płynnie przeszłam do kontaktu z klientami, już jako pracownik kontraktowy, zajmując się wsparciem w procesie zakupu przez nich sprzętu. Szczególną satysfakcję czerpię z obszaru sprzedaży falowników oraz produktów naszej własnej marki, Astraada. Obecnie mam zamiar podążać nieco inną ścieżką i dążyć do osiągnięcia nowych celów, zajmując się dystrybucją robotów Kawasaki oraz opiekując się sektorem edukacji oraz promowaniem robota Astorino. Nie mogę się doczekać nowych wyzwań, jakie przyniesie mi ta fascynująca droga, wraz z wspaniałym zespołem.

W wolnym czasie chętnie odwiedzam siłownię lub, przy ładnej pogodzie, spaceruję, odkrywając nowe zakątki mojej okolicy.

Spędzam także wieczory przy planszówkach lub grze w pokera, razem z grupą licealnych przyjaciół. Aby oderwać się od inżynieryjnego świata, wnikam w świat sztuki, podziwiając dzieła wybitnych artystów. Szczególnie urzekł mnie okres impresjonizmu, który poznałam, zwiedzając Musée du Louvre i Musée d'Orsay w Paryżu. •

Waldemar Sadowski

Dyrektor ds. administracji

Cześć!

W firmie ASTOR pracuję od 2018 roku. Wcześniej – w 2003 roku – ukończyłem automatykę i robotykę na Politechnice Krakowskiej i…założyłem własną firmę w kompletnie innej branży :)

Zajmowałem się kompleksową obsługą inwestycji budowlanych a w tym: weryfikacją i obliczeniami dotyczącymi konstrukcji budowlanych, domów, kompleksowe wykonawstwo prac termoizolacyjnych, sprzedaż hurtowa i detaliczna materiałów budowlanych itp. Przygoda ta trwała ponad 12 lat. Przez ten czas zdobyłem mnóstwo doświadczenia w różnych obszarach, od kontaktu z klientem przez logistykę, administrację po zarządzanie zespołem/zespołami ludzi. Od 2015 roku zacząłem się zastanawiać, czy mam szansę zrobić w życiu tzw. drugie okrążenie i wrócić do swojej wyuczonej branży. Walka z samym sobą trwała do 2016 roku, kiedy to zakończyłem etap własnej działalności i postanowiłem wrócić do automatyki i robotyki. Przez dwa lata pracowałem w kilku firmach w Polsce i za granicą, mniej lub bardziej związanych z automatyzacją procesów produkcyjnych, ale…czułem że to nie to.

Dopiero rok 2018 okazał się przełomowy – i znalazłem się w ASTORZE. Na początku jako koordynator ds. administracji, później doszła koordynacja sprzedaży usług w robotyce, a obecnie prowadzę pion wsparcia składający się z dwóch działów, są to: dział realizacji zamówień robotyki oraz dział administracji ASTOR. Mogę śmiało powiedzieć, że zawodowo w znalazłem tu swoje miejsce, mam świetny zespół ludzi, z którymi współpracuję, nie brakuje wyzwań, rozwoju osobistego, a to dla mnie bardzo ważne. Utożsamiam się z misją, wizją i wartościami firmy, więc tym bardziej praca tutaj daje mi dużo satysfakcji i spełnienia zawodowego.

Prywatnie również nie lubię nudy, więc moją pasją jest sport. Poza tym, że oglądam i czytam :), to również aktywnie uprawiam. Bardzo lubię pobiegać, poćwiczyć na siłowni, pograć w piłkę nożną – czasami tydzień jest za krótki na te wszystkie aktywności, ale staram się jakoś to pogodzić :).

Ponadto bardzo lubimy weekendowe wypady z rodzinką (żoną i córką) w góry, a jeżeli pogoda nieodpowiednia, to chętnie odwiedzamy też kino, teatr czy dobry kabaret – ładujemy wówczas baterie na cały kolejny tydzień. •

ASTRAADA

Automatyka?
U nas bezproblemowa!

Sprawdź ofertę Astraady

Szeroka oferta

Wsparcie techniczne

Zamienniki na czas serwisu

Sprawdź:
astraada.com