

TELEMETRON

Cyberodporna telemetria
dla branży wod-kan

strona 4

Praktyczny przewodnik po
wymaganiach, kryteriach
oceny ofert i dostawców

strona 8

Pakiety telemetryczne
dla branży wod-kan

strona 23

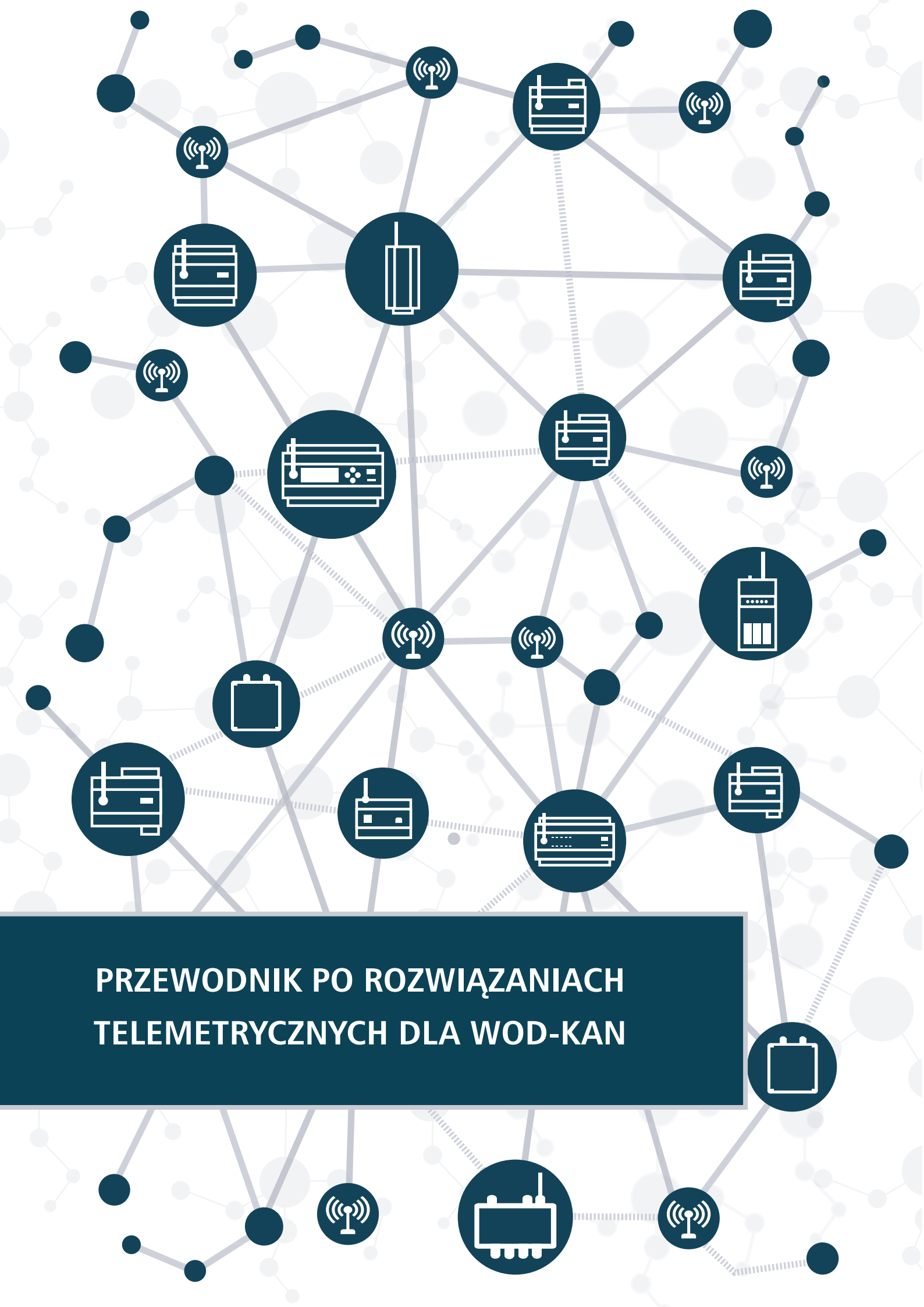
Regulacje i standardy
istotne dla cyberodpornej
telemetrii wod-kan

strona 52

MAGAZYN TELEMTRYCZNY

poświęcony profesjonalnym rozwiązaniom IoT dla branży wod-kan





PRZEWODNIK PO ROZWIĄZANIACH TELEMETRYCZNYCH DLA WOD-KAN



Szanowni Państwo,

przedsiębiorstwa wodociągowo-kanalizacyjne od lat odpowiadają za usługi, których znaczenie trudno przecenić: ciągłość dostaw wody, odbiór i oczyszczanie ścieków, bezpieczeństwo mieszkańców, ochronę środowiska oraz sprawne zarządzanie infrastrukturą rozproszoną.

W ostatnim czasie zmienia się jednak otoczenie, w którym funkcjonuje branża wod-kan. Regulacje takie jak NIS2, Cyber Resilience Act, RED-DA, CER, przepisy dotyczące jakości wody przeznaczonej do spożycia oraz poprawy dostępu do wody, a także dobre praktyki wynikające m.in. z IEC 62443 powodują, że coraz większe znaczenie ma nie tylko to, czy system działa, ale również czy jest bezpieczny, aktualizowany, wspierany, udokumentowany i możliwy do utrzymania przez cały cykl życia.

Nie oznacza to, że każde przedsiębiorstwo musi natychmiast wymieniać całą infrastrukturę lub wdrażać kosztowne, przewymiarowane rozwiązania. Oznacza jednak, że warto świadomie spojrzeć na obecnie eksploatowane systemy telemetryczne, sposób zarządzania dostępem do infrastruktury, jakość danych, dostawców, usługi cyfrowe oraz możliwość dokumentowania zdarzeń i reakcji.

W przypadku wodociągów dane z obiektów terenowych mają znaczenie nie tylko eksploatacyjne. Coraz częściej wspierają także zarządzanie ryzykiem jakości wody, ciągłością dostaw, dostępnością usług, bezpieczeństwem infrastruktury oraz dokumentowaniem działań podejmowanych w przypadku awarii, incydentu lub sytuacji kryzysowej.

Z naszej perspektywy telemetria przestała być wyłącznie narzędziem zdalnego odczytu lub wygodniejszej eksploatacji obiektów terenowych. Stała się jednym z elementów cyberodporności, ciągłości działania i zarządzania ryzykiem w infrastrukturze wodociągowo-kanalizacyjnej. I to elementem nader istotnym.

Inventia od 25 lat rozwija rozwiązania telemetryczne dla infrastruktury rozproszonej, przemysłu i branży wod-kan. Jesteśmy polską firmą, a projektowanie i produkcja naszych urządzeń odbywają się w Polsce. Dzięki temu możemy zapewniać bezpośredni kontakt z producentem, lokalne wsparcie techniczne oraz lepsze zrozumienie realiów krajowej infrastruktury wodociągowo-kanalizacyjnej. Nasza wieloletnia obecność w tym sektorze została w 2026 roku dostrzeżona również przez środowisko branżowe - podczas Targów Wod-Kan w Bydgoszczy otrzymaliśmy list gratulacyjny od Izby Gospodarczej „Wodociągi Polskie”, podpisany przez Prezesa Izby.

Traktujemy to wyróżnienie jako powód do dumy, ale również jako zobowiązanie. Jest ono spójne z misją, którą Inventia od lat konsekwentnie realizuje: **wspieranie przedsiębiorstw infrastrukturalnych w niezawodnym, bezpiecznym i odpowiedzialnym nadzorze nad obiektami rozproszonymi.** Dziś oznacza to nie tylko dostarczanie urządzeń telemetrycznych, ale także pomoc w budowaniu odporności, ciągłości działania i świadomego podejścia do ryzyka technologicznego.

Dlatego pod znanym od lat szyldem „Telemetron” przygotowaliśmy dla Państwa krótki materiał informacyjny poświęcony cyberodpornej teledzielnictwu w branży wod-kan. Nie jest to opinia prawna ani audyt bezpieczeństwa. Jest to praktyczny przewodnik edukacyjny, który ma pomóc uporządkować najważniejsze pytania, jakie warto zadać przy modernizacji, zakupie lub ocenie systemu teledzielnictwa.

W materiale zwracamy uwagę m.in. na:

- znaczenie teledzielnictwa jako elementu ciągłości działania przedsiębiorstwa wod-kan,
- ryzyka związane z eksploatacją rozproszonej infrastruktury technicznej,
- wpływ nowych regulacji na ocenę systemów, dostawców i usług cyfrowych,
- rolę danych, alarmów i historii zdarzeń w podejmowaniu decyzji oraz wykazywaniu należytej staranności,
- znaczenie odpowiedzialnego wyboru dostawcy technologii, który zapewnia wsparcie, aktualizacje i utrzymanie rozwiązania w całym cyklu życia produktu,
- potrzebę oceny nie tylko urządzeń terenowych, ale również transmisji danych, systemów nadrzędnych, usług chmurowych i dostępu zdalnego,
- praktyczne pytania, które warto zadać przed modernizacją, zakupem lub oceną obecnego systemu teledzielnictwa.

Chcemy, aby zebrany materiał pomógł spojrzeć na teledzielnictwo nie tylko jako na element automatyki, ale także jako na narzędzie zarządzania ryzykiem, ciągłością działania, jakością usług i odpowiedzialnością za decyzje podejmowane na podstawie danych z infrastruktury terenowej.

Naszym celem nie jest budowanie przekazu opartego na strachu przed regulacjami. Chcemy pokazać, że cyberodporność można i należy budować rozsądnie – przez wiedzę, właściwe wymagania, dobrą architekturę, kontrolę dostępu, aktualizacje, dokumentację i wybór odpowiedzialnych dostawców. W tym podejściu szczególnie ważne są standardy zarządzania bezpieczeństwem informacji, takie jak ISO 27001, które porządkują sposób identyfikowania ryzyk, wdrażania zabezpieczeń, nadzorowania procesów i ciągłego doskonalenia ochrony danych oraz systemów. Inwentia ten wysiłek już podjęła: proces przygotowania do certyfikacji wymagał uporządkowania procedur, przeglądu uprawnień, wzmocnienia dokumentacji, oceny ryzyk oraz zaangażowania zespołów w codzienną praktykę bezpieczeństwa.

Z końcem 2025 roku Inwentia uzyskała certyfikat ISO 27001. Traktujemy go nie jako jednorazowe osiągnięcie, lecz jako potwierdzenie kierunku, który od lat rozwijamy: odpowiedzialnego projektowania, produkcji, wsparcia i utrzymania rozwiązań teledzielnictwa dla infrastruktury rozproszonej. Z perspektywy Klientów ma to bardzo konkretne znaczenie. Odpowiedzialny dostawca nie tylko dostarcza technologię, ale także wspiera Klienta w utrzymaniu zgodności, przejrzystości dokumentacji, bezpiecznym zarządzaniu zmianą, obsłudze aktualizacji i reagowaniu na incydenty. Dostawca, który świadomie inwestuje w bezpieczeństwo informacji, lepiej chroni ciągłość swojej działalności, ogranicza ryzyko przerw operacyjnych, zapewnia bardziej przewidywalne wsparcie i skuteczniej chroni informacje powierzane mu w ramach wspólnych projektów.

Dlatego patrzymy na cyberodporność nie jak na jednorazowe wdrożenie, lecz jak na proces stałego doskonalenia. W branży wodociągowo-kanalizacyjnej, gdzie niezawodność systemów, jakość danych i ciągłość działania mają bezpośrednie znaczenie dla bezpieczeństwa mieszkańców oraz funkcjonowania infrastruktury krytycznej, takie podejście staje się szczególnie istotne.

Zachęcamy do zapoznania się z materiałem i wykorzystania go jako punktu wyjścia do rozmów wewnętrznych, z projektantami, integratorami oraz dostawcami systemów teledzielnictwa.

Z poważaniem,
Jerzy Białousz - Prezes Zarządu Inwentia Sp. z o.o.

Spis treści	Strona
Słowo wstępu	1-2
Spis treści	3
Cyberodporna teledzielnictwa dla branży wod-kan	4-7
Praktyczny przewodnik po wymaganiach, kryteriach oceny ofert i dostawców	8-17
DataPortal – platforma zdalnego nadzoru, wizualizacji i alarmowania dla teledzielnictwa wod-kan	18-22
Pakiety teledzielnictwa dla branży wod-kan	23-29
MT-121 – Sterownik teledzielnictwa programowany w środowisku CODESYS®	30-31
MT-151 HMI – Sterownik teledzielnictwa programowany w środowisku CODESYS®	32-33
MT-151 LED – Sterownik teledzielnictwa programowany w środowisku CODESYS®	34-35
MT-025 v3 – Ekonomiczny moduł teledzielnictwa	36-37
MT-718 PS – baterijny, energooszczędny moduł rejestrujący z IP68	38-39
MT-058 – baterijny moduł teledzielnictwa z IP68	40-41
MT-221 – Brama komunikacyjna programowana w środowisku CODESYS®	42-43
MTX-2050 v4 – 2G/LTE brama komunikacyjna z portem Ethernet	44-46
Akcesoria do modułów	47-48
Zastosowania teledzielnictwa w branży wod-kan	49-51
Regulacje i standardy istotne dla cyberodpornej teledzielnictwa wod-kan	52-57
Porównanie cech modułów teledzielnictwa dedykowanych branży wod-kan (tabela)	58-59
Dlaczego Inwentia?	60-63



Cyberodporna telemetria dla branży wod-kan

Telemetria w przedsiębiorstwach wodociągowo-kanalizacyjnych coraz częściej przestaje być jedynie narzędziem zdalnego odczytu i bieżącej eksploatacji.

W obliczu rosnących wymagań dotyczących ciągłości działania, cyberbezpieczeństwa, zarządzania ryzykiem i odpowiedzialności dostawców staje się ważnym elementem odporności całej organizacji. Poniższy materiał wskazuje kluczowe obszary, które warto przeanalizować przy ocenie, modernizacji lub wyborze systemu telemetrycznego, aby rozwiązanie było nie tylko funkcjonalne, ale także bezpieczne, udokumentowane i możliwe do utrzymania przez cały cykl życia.

Kluczowe obszary, które warto sprawdzić przy modernizacji lub ocenie systemu telemetrycznego

1. Dlaczego warto spojrzeć na telemetrię szerzej?

Przedsiębiorstwa wodociągowo-kanalizacyjne zarządzają infrastrukturą rozproszoną: ujęciami wody, stacjami uzdatniania, przepompowniami, oczyszczalнями, zbiornikami, punktami pomiarowymi, komorami, zasuwami, przelewami i instalacjami terenowymi.

Część tych obiektów pracuje bez stałej obecności obsługi. Część znajduje się w trudno dostępnych lokalizacjach. W wielu przypadkach decyzja operacyjna zależy od tego, czy informacja z obiektu dotrze szybko, wiarygodnie i w sposób możliwy do odtworzenia.

Dlatego telemetria nie jest już wyłącznie narzędziem zdalnego odczytu lub wygodniejszej eksploatacji. Coraz częściej staje się elementem ciągłości działania, cyberodporności, zarządzania ryzykiem, kontroli dostawców, jakości danych i dokumentowania reakcji na zdarzenia.

Regulacje takie jak NIS2, Cyber Resilience Act (CRA), Critical Entities Resilience (CER), przepisy dotyczące jakości wody przeznaczonej do spożycia oraz poprawy dostępu do wody, a także dobre praktyki wynikające m.in. z IEC 62443, EN 18031 i ISO/IEC 27001, nie nakazują zakupu konkretnego systemu telemetrycznego. Zmieniają jednak sposób,

w jaki należy patrzeć na infrastrukturę, dostawców, dane, dostęp zdalny, usługi cyfrowe, aktualizacje, dokumentację i możliwość wykazania należytej staranności.

Najważniejsze pytanie nie brzmi już tylko:

Ile kosztuje urządzenie?

Coraz częściej powinno brzmieć:

Czy ten system będzie możliwy do bezpiecznego utrzymania, aktualizowany, wspierany, udokumentowany i możliwy do obrony przez cały cykl życia?

Cyberodporna telemetria to temat zarządczy, nie tylko techniczny

Cyberbezpieczeństwo systemów telemetrycznych, SCADA, usług chmurowych i dostawców technologii nie jest już wyłącznie zagadnieniem technicznym. W realiach NIS2 i krajowych przepisów dotyczących cyberbezpieczeństwa kierownictwo organizacji powinno rozumieć ryzyko, nadzorować środki zarządzania bezpieczeństwem, zapewniać odpowiednie zasoby oraz móc wykazać, że decyzje dotyczące infrastruktury, dostawców i utrzymania systemów były podejmowane świadomie.

W określonych przypadkach odpowiedzialność może dotyczyć nie tylko samego podmiotu, ale również osób kierujących organizacją. Dlatego wybór i utrzymanie systemu telemetrycznego warto traktować jako element zarządzania ryzykiem, ciągłością działania i należytą starannością, a nie wyłącznie jako decyzję techniczną lub zakupową.

2. Własna SCADA, platforma zdalnego nadzoru i podział odpowiedzialności

Wiele przedsiębiorstw wodociągowo-kanalizacyjnych korzysta z „własnych” systemów SCADA, serwerów, baz danych i lokalnych środowisk wizualizacji. Takie podejście daje dużą kontrolę nad systemem, ale oznacza również pełną odpowiedzialność za jego bezpieczne utrzymanie.

W realiach NIS2, CRA i rosnących wymagań wobec dostawców technologii warto zadać sobie pytanie, czy organizacja jest gotowa samodzielnie zapewnić i udokumentować kluczowe obszary związane z utrzymaniem takiego systemu. W przypadku własnego środowiska SCADA kluczowe nie jest tylko to, czy system działa dzisiaj. Równie ważne jest to, czy przedsiębiorstwo potrafi bezpiecznie utrzymać go przez kolejne lata i wykazać, że najważniejsze obszary są objęte nadzorem.

W praktyce warto wiedzieć m.in.:

- kto odpowiada za aktualizację systemu, baz danych, komponentów SCADA i powiązanych usług i czy okresowo wykonuje te czynności,
- czy używane komponenty są cyklicznie sprawdzane pod kątem podatności i końca wsparcia,
- czy system jest objęty kopiami zapasowymi oraz testami odtworzeniowymi,
- czy dostęp administratorów, integratorów i użytkowników jest kontrolowany, rejestrowany i regularnie weryfikowany,
- czy wykonywane są okresowe przeglądy konfiguracji lub testy bezpieczeństwa tam, gdzie jest to uzasadnione,
- czy istnieje procedura reagowania na incydenty, np. dotyczące systemu SCADA,
- kto odpowiada za utrzymanie systemu po zmianie integratora, administratora lub dostawcy.

To nie są wyłącznie kwestie techniczne. To elementy, które mogą mieć znaczenie podczas audytu, kontroli, analizy incydentu lub oceny należytej staranności po stronie przedsiębiorstwa i kadry zarządzającej.

W tym miejscu warto rozważyć rolę platform zdalnego nadzoru i usług chmurowych wspierających telemetrię. Takie rozwiązania mogą ograniczyć część obowiązków związanych z utrzymaniem własnej infrastruktury serwerowej, aktualizacjami, dostępnością, kopiami zapasowymi, odtwarzaniem, zarządzaniem użytkownikami i rejestrowaniem zdarzeń.

Platforma zdalnego nadzoru nie zastępuje analizy ryzyka po stronie przedsiębiorstwa i nie zwalnia użytkownika z odpowiedzialności za właściwą konfigurację, zarządzanie dostępami oraz organizację pracy. Może jednak stanowić element uporządkowanego ekosystemu telemetrycznego, w którym część odpowiedzialności technicznej i utrzymaniowej jest realizowana przez wyspecjalizowanego dostawcę.

Przykładem takiego rozwiązania w ekosystemie Inventii jest DataPortal

Dla zarządu przedsiębiorstwa wod-kan istotne pytanie nie brzmi więc wyłącznie:

Czy mamy system SCADA?

Równie ważne pytanie brzmi:

Czy jesteśmy w stanie bezpiecznie utrzymać, aktualizować, testować, dokumentować i audytować ten system przez kolejne lata?

3. Sześć obszarów cyberodpornej telemetrii

OBSZAR	DLACZEGO JEST WAŻNY
1. Ciągłość działania	Telemetria pomaga szybciej wykrywać awarie, zakłócenia i nietypowe stany na obiektach rozproszonych. Brak informacji może wydłużyć czas reakcji i zwiększyć skutki awarii.
2. Dane, alarmy i historia zdarzeń	Dane z systemu telemetrycznego wspierają decyzje operacyjne, analizę awarii, obsługę reklamacji, audyty oraz udowadnianie należytej staranności.
3. Dostęp do systemów i odpowiedzialność	Dostęp do telemetrii, SCADA, usług cyfrowych i funkcji sterujących powinien być kontrolowany, uzasadniony i możliwy do rozliczenia zgodnie z polityką organizacji.
4. Dostawca i cykl życia rozwiązania	Wybór dostawcy to decyzja na lata. Znaczenie ma nie tylko cena zakupu, ale również wsparcie, aktualizacje, dokumentacja, rozwiązywanie podatności i możliwość utrzymania systemu w czasie.
5. SCADA, platforma zdalnego nadzoru i utrzymanie systemu	Własna infrastruktura daje kontrolę, ale oznacza także odpowiedzialność za aktualizacje, kopie zapasowe, odtwarzanie, bezpieczeństwo, testy i dokumentację. Platforma zdalnego nadzoru może część tych obszarów porządkować, ale nie zwalnia zamawiającego z analizy ryzyka i właściwej organizacji pracy.
6. Dokumentacja, kopie zapasowe i odtworzenie	Brak aktualnej dokumentacji i kopii konfiguracji może wydłużyć czas usunięcia awarii z godzin do dni. Dokumentacja jest ważna także po zmianie integratora, administratora lub modelu utrzymania systemu.

4. Cena zakupu to nie cały koszt systemu

Przy porównywaniu ofert warto patrzeć nie tylko na cenę urządzenia lub wdrożenia. W całym cyklu życia systemu znaczenie mają również koszty i ryzyka związane z utrzymaniem, integracją, aktualizacjami, serwisem, dokumentacją, dostępnością części, licencjami, odświeżaniem lub wymianą infrastruktury serwerowej, usługami dodatkowymi i czasem reakcji.

Tanie rozwiązanie może okazać się drogie, jeżeli wymaga wielu dodatkowych elementów, częstych interwencji, trudnej integracji, ręcznej diagnostyki, dodatkowych licencji, indywidualnych prac serwisowych lub kosztownej modernizacji po kilku latach.

Warto więc pytać nie tylko:

Ile kosztuje zakup?

Ale również:

Ile będzie kosztować bezpieczne utrzymanie tego systemu przez kolejne lata?

5. Od czego zacząć?

10 pytań do szybkiej diagnozy

Cyberodporność telemetrii nie musi zaczynać się od dużej inwestycji. Często pierwszym krokiem jest uporządkowanie wiedzy o obecnym systemie oraz wskazanie miejsc, w których ryzyko jest największe. Takie działania pozwala stworzyć plan mitygacji ryzyka, umożliwiając skupienie często ograniczonych sił i środków na tych najistotniejszych obszarach.

Warto zacząć od odpowiedzi na 10 pytań:

1. Czy wiemy, które obiekty terenowe są najważniejsze dla zapewnienia ciągłości działania?
2. Czy mamy aktualną listę urządzeń telemetrycznych, ich lokalizacji, wersji oprogramowania i statusu wsparcia?
3. Czy wiemy, kto ma dostęp do systemu, danych, urządzeń i funkcji sterujących?
4. Czy system pozwala odtworzyć historię alarmów, działań użytkowników i zmian konfiguracji?
5. Czy wiemy, jak postępować w przypadku braku łączności, niedostępności SCADA, awarii platformy lub utraty danych z obiektu?
6. Czy dostawca zapewnia wsparcie, aktualizacje,

obsługę podatności i jasny cykl życia produktu lub usługi?

7. Czy system będzie możliwy do utrzymania po zmianie integratora lub administratora?
8. Czy własna SCADA lub lokalna infrastruktura serwerowa są objęte aktualizacjami, kopiami zapasowymi, testami i nadzorem bezpieczeństwa?
9. Czy usługi chmurowe, transmisja danych i dostęp zdalny są objęte oceną ryzyka oraz mają opisany podział odpowiedzialności?
10. Czy decyzja zakupowa da się obronić nie tylko technicznie i cenowo, ale również z punktu widzenia ryzyka, ciągłości działania i należytej staranności?

6. Podsumowanie

Cyberodporna telemetria nie jest pojedynczą funkcją urządzenia ani jedną usługą. Jest wynikiem właściwego połączenia produktu, architektury, transmisji danych, systemu nadrzędnego, usług cyfrowych, polityk i procedur, aktualizacji, dostępu, dokumentacji, kopii zapasowych i odpowiedzialnego dostawcy.

Widzieć wcześniej.
Reagować szybciej.
Dokumentować lepiej.

Materiał informacyjny dla przedsiębiorstw wodociągowo-kanalizacyjnych

Opracowanie: Inventia Sp. z o.o.

© 2026 Inventia Sp. z o.o.

Wszelkie prawa zastrzeżone.

Niniejszy materiał ma charakter informacyjny i edukacyjny. Nie stanowi opinii prawnej, audytu bezpieczeństwa, dokumentacji projektowej ani instrukcji zapewnienia zgodności z regulacjami. Decyzje dotyczące projektowania, zakupu, modernizacji i utrzymania systemów telemetrycznych powinny być podejmowane z uwzględnieniem indywidualnej analizy ryzyka, specyfiki organizacji, obowiązujących przepisów oraz wymagań technicznych danego systemu.

Najważniejsze korzyści



Praktyczny przewodnik po wymaganiach, kryteriach oceny ofert i dostawców

Materiał pomocniczy dla przedsiębiorstw wodociągowo-kanalizacyjnych, projektantów i integratorów.

1. Cel artykułu

Celem artykułu jest wskazanie, na jakie obszary cyberodporności warto zwracać uwagę przy projektowaniu, zakupie, modernizacji i utrzymaniu systemów telemetrycznych w przedsiębiorstwach wodociągowo-kanalizacyjnych.

Artykuł może być wykorzystany jako materiał pomocniczy przy przygotowywaniu wymagań technicznych, dokumentacji projektowej, opisu przedmiotu zamówienia, specyfikacji warunków zamówienia, kryteriów oceny ofert, rozmów z dostawcami oraz odbioru wdrożonego rozwiązania.

Artykuł nie jest gotowym OPZ ani gotową SWZ. Jest katalogiem zagadnień, które warto rozważyć przy projektach dotyczących urządzeń telemetrycznych, sterowników telemetrycznych, modułów komunikacyjnych, transmisji danych, systemów zdalnego nadzoru, usług chmurowych, integracji z systemami SCADA oraz utrzymania i modernizacji systemów telemetrycznych.

Celem nie jest wprowadzenie nadmiernie rozbudowanych wymagań formalnych. Celem jest takie ukształtowanie projektu i postępowania, aby Zamawiający mógł świadomie ocenić nie tylko cenę, ale również dojrzałość rozwiązania, cykl życia produktu, bezpieczeństwo transmisji, aktualizacje, obsługę podatności, odpowiedzialność w łańcuchu dostaw, wsparcie techniczne oraz możliwość utrzymania rozwiązania przez lata.

Regulacje i standardy, które mogą mieć znaczenie dla cyberodpornej telemetrii wod-kan, zostały omówione w osobnym przyborniku regulacyjno-normatywnym. Niniejszy artykuł nie powiela tego omówienia. Koncentruje się na praktycznych wymaganiach, kryteriach oceny i pytaniach, które można wykorzystać przy przygotowywaniu dokumentacji projektowej, OPZ, SWZ, rozmów z dostawcami i odbioru wdrożonego rozwiązania.

2. Terminologia

Na potrzeby niniejszego artykułu pojęcie „dostawca” oznacza podmiot oferujący, dostarczający lub utrzymujący element systemu telemetrycznego. Może to być w szczególności producent urządzeń, producent oprogramowania, dystrybutor, integrator, partner wdrożeniowy, dostawca usługi chmurowej, dostawca transmisji danych lub podmiot świadczący usługi serwisowe.

W praktyce role te mogą być wykonywane przez jeden podmiot albo przez kilka podmiotów działających w łańcuchu dostaw. Dlatego w projektach telemetrycznych istotne jest nie tylko to, kto składa ofertę, ale również kto jest producentem urządzeń, kto odpowiada za firmware, kto obsługuje aktualizacje i podatności, kto świadczy usługę oraz kto zapewnia wsparcie techniczne.

W przykładowych zapisach do OPZ/SWZ używane jest pojęcie „Wykonawca”, ponieważ odpowiada ono typowemu językowi dokumentacji zakupowej i przetargowej.

3. Podstawowa zasada

Cyberodporność w projekcie telemetrycznym nie powinna polegać na przepisaniu długiej listy zabezpieczeń technicznych. W praktyce dużo ważniejsze jest, aby Zamawiający potrafił ocenić, czy oferowane rozwiązanie będzie możliwe do bezpiecznego utrzymania w całym cyklu życia.

Dlatego przy projektowaniu, zakupie i ocenie rozwiązań telemetrycznych warto zwracać uwagę na cały ekosystem:

- kto jest faktycznym producentem urządzeń i oprogramowania,
- kto odpowiada za firmware i aktualizacje,
- jaka jest rola wykonawcy w łańcuchu dostaw,
- czy istnieje proces obsługi podatności,
- czy transmisja danych jest właściwie zabezpieczona,
- czy firmware i proces aktualizacji są zabezpieczone adekwatnie do funkcji urządzenia,
- czy dostawca posiada adekwatne procesy bezpieczeństwa,

- czy usługi chmurowe mają opisany podział odpowiedzialności,
- czy Zamawiający otrzyma wsparcie pozwalające utrzymać albo nadzorować system po wdrożeniu, a w przypadku usług chmurowych – informacje potrzebne do oceny, nadzoru w czasie ewentualnego audytu,
- czy Zamawiający wie, kto odpowiada za utrzymanie rozwiązania oraz jak zapewnić ciągłość eksploatacji w przypadku zmiany integratora, administratora lub modelu korzystania z usługi.

Dobrze przygotowane wymagania nie powinny przerzucać całej odpowiedzialności na wykonawcę. Powinny natomiast pomagać wybrać dostawcę i rozwiązanie, które ułatwią Zamawiającemu zarządzanie ryzykiem, ciągłością działania, łańcuchem dostaw i należyтым utrzymaniem systemu.

4. Jak korzystać z artykułu?

Wymagania opisane w niniejszym materiale należy traktować jako katalog zagadnień do rozważenia, a nie jako obowiązkową listę warunków do bezpośredniego przepisania do każdego OPZ lub SWZ.

Zakres wymagań powinien być dostosowany do rodzaju projektu, modelu dostawy, znaczenia systemu, funkcji rozwiązania oraz poziomu ryzyka. Inaczej należy traktować dostawę urządzeń, inaczej wdrożenie systemu telemetrycznego u Zamawiającego, a inaczej usługę chmurową, platformę zdalnego nadzoru, usługę cyfrową wspierającą telemetrię albo model abonamentowy.

Wymagania dotyczące produktu, firmware, aktualizacji, podatności, cyklu życia lub certyfikacji mogą być potwierdzane nie tylko przez integratora lub dystrybutora, ale również przez producenta urządzeń, producenta oprogramowania, dostawcę usługi lub inny podmiot odpowiedzialny za dany element rozwiązania.

Celem artykułu nie jest obciążanie podmiotów nadmierną dokumentacją ani wymaganie od nich odpowiedzialności za obszary, na które nie mają bezpośredniego wpływu. Celem jest zapewnienie przejrzystości: kto jest producentem, kto odpowiada za rozwój i utrzymanie produktu, kto obsługuje aktualizacje i podatności, kto świadczy usługę oraz jak Zamawiający może bezpiecznie korzystać z rozwiązania w całym cyklu życia.

5. Co powinno pozostać po stronie polityki Zamawiającego?

Nie wszystkie elementy cyberodporności powinny być wpisywane jako wymaganie wobec wykonawcy.

Znaczna część cyberodporności całego systemu zależy od polityki, architektury i decyzji samego przedsiębiorstwa wod-kan.

Dotyczy to w szczególności:

- wewnętrznej polityki dostępu zdalnego,
- decyzji, kto zatwierdza dostęp serwisowy,
- zasad nadawania i odbierania uprawnień pracownikom,
- segmentacji istniejącej sieci zakładowej,
- zarządzania własnym systemem SCADA,
- częstotliwości wewnętrznych audytów,
- organizacji procesu reagowania na incydenty,
- zasad współpracy z własnym działem IT, automatyką i utrzymaniem ruchu.

W takich przypadkach dokumentacja projektowa lub zakupowa powinna raczej wymagać, aby projektant lub wykonawca:

- dostosował się do polityki Zamawiającego,
- opisał założenia techniczne,
- wskazał wymagane dostępy,
- umożliwił ograniczenie dostępow,
- przekazał informacje adekwatne do swojej roli,
- wskazał ograniczenia i ryzyka,
- określił zakres odpowiedzialności po swojej stronie.

Przykład

Zamawiający powinien wymagać, aby zdalny dostęp serwisowy do urządzeń, systemu lub usługi był realizowany wyłącznie w sposób kontrolowany, uzasadniony, ograniczony czasowo i zakresowo oraz możliwy do udokumentowania. Wykonawca powinien opisać proponowany sposób realizacji dostępu, wymagane uprawnienia, mechanizm jego uruchamiania i zamykania, zasady rejestrowania czynności serwisowych oraz ograniczenia i ryzyka związane z przyjętym rozwiązaniem.

6. Co warto uwzględnić jako wymagania minimalne?

Wymagania minimalne powinny określać podstawowy poziom przejrzystości, utrzymaniowości i odpowiedzialności w łańcuchu dostaw. Nie powinny być nadmiernie rozbudowane, ale powinny skłaniać do ujawnienia najważniejszych informacji o produkcie, usłudze i modelu utrzymania.

6.1. Producent, pochodzenie rozwiązania i odpowiedzialność w łańcuchu dostaw

Zamawiający powinien wymagać, aby w ofercie lub dokumentacji rozwiązania wskazano:

- producenta urządzeń,
- producenta oprogramowania lub firmware,
- czy oferowane rozwiązanie jest produktem własnym producenta, produktem OEM, tzw. white label lub rozwiązaniem podmiotu trzeciego oferowanym pod marką dostawcy,
- rolę wykonawcy w łańcuchu dostaw, w szczególności czy występuje jako producent, autoryzowany dystrybutor, integrator, partner wdrożeniowy lub dostawca usługi,
- podmiot odpowiedzialny za rozwój, utrzymanie, aktualizacje i obsługę podatności oferowanego rozwiązania,
- sposób zapewnienia współpracy z producentem lub podmiotem odpowiedzialnym za utrzymanie produktu,
- czy wykonawca posiada dokumentację, upoważnienie, umowę partnerską, kanał wsparcia lub inny mechanizm współpracy, umożliwiający skuteczne wsparcie produktu w deklarowanym okresie eksploatacji.

Przykład

Wykonawca wskaże producenta oferowanych urządzeń, oprogramowania lub firmware oraz opíše swoją rolę w łańcuchu dostaw. Jeżeli Wykonawca nie jest producentem oferowanego rozwiązania, powinien wskazać podmiot odpowiedzialny za rozwój, aktualizacje, obsługę podatności, dokumentację techniczną oraz wsparcie produktu, a także opisać sposób współpracy z tym podmiotem.

Jeżeli oferowane urządzenie jest produktem OEM, white label lub produktem wytwarzanym przez podmiot trzeci, Wykonawca powinien wykazać, że posiada skuteczny mechanizm współpracy z producentem lub podmiotem odpowiedzialnym za produkt, umożliwiający obsługę aktualizacji, podatności, dokumentacji technicznej oraz wsparcia produktu w deklarowanym okresie eksploatacji.

6.2. Oświadczenie lub inne potwierdzenie dotyczące nieudokumentowanych mechanizmów dostępu

W przypadku urządzeń telemetrycznych, sterowników, modułów komunikacyjnych i usług zdalnych warto ograniczać ryzyko nieudokumentowanych dostępow serwisowych lub funkcji komunikacyjnych.

Nie oznacza to, że każdy integrator lub dystrybutor musi samodzielnie weryfikować firmware i hardware oferowanego produktu. W zależności od modelu dostawy potwierdzenie może pochodzić od producenta, dostawcy usługi lub innego podmiotu odpowiedzialnego za dany element rozwiązania.



Przykład

Wykonawca powinien przedstawić, w zakresie adekwatnym do swojej roli w łańcuchu dostaw, informacje lub dokumenty potwierdzające, że oferowane urządzenia, oprogramowanie lub usługi są rozwijane i utrzymywane w sposób ograniczający ryzyko nieudokumentowanych mechanizmów dostępu, kont serwisowych, funkcji komunikacyjnych lub innych mechanizmów umożliwiających nieautoryzowany dostęp do urządzenia, danych lub systemu Zamawiającego.

Potwierdzenie może mieć w szczególności formę oświadczenia producenta, dostawcy usługi lub podmiotu odpowiedzialnego za dany element rozwiązania, opisu mechanizmów kontroli dostępu, dokumentacji bezpieczeństwa produktu, deklaracji producenta, dokumentacji zgodności z właściwymi wymaganiami produktowymi, jeżeli mają zastosowanie.

6.3. Cykl życia i wsparcie produktu

Zamawiający powinien oczekiwać informacji o tym, jak długo produkt lub usługa będą wspierane oraz jak wygląda ścieżka aktualizacji i zakończenia wsparcia.

W przypadku produktów z elementami cyfrowymi określenie okresu wsparcia będzie jednym z istotnych obowiązków wynikających z regulacji produktowych dotyczących cyberodporności. Do czasu pełnego stosowania tych wymagań wskazanie dekla-

rowanego okresu wsparcia warto traktować jako element należytej staranności, oceny utrzymywaności rozwiązania oraz przygotowania do przyszłych wymagań rynkowych i regulacyjnych.

W zależności od modelu dostawy informacje te mogą pochodzić od producenta, dystrybutora, integratora, dostawcy usługi lub innego podmiotu odpowiedzialnego za utrzymanie rozwiązania.

Warto określić:

- deklarowany okres wsparcia produktu lub usługi,
- zasady informowania o końcu wsparcia,
- możliwość aktualizacji firmware lub oprogramowania,
- sposób informowania o aktualizacjach,
- zasady wsparcia po wdrożeniu,
- możliwość migracji po zakończeniu wsparcia.

Przykład

Wykonawca wskaże deklarowany okres wsparcia oferowanych urządzeń, oprogramowania lub usług oraz opíše zasady informowania Zamawiającego o aktualizacjach, zmianach, końcu wsparcia i zalecanej ścieżce migracji. Informacje te mogą wynikać z dokumentacji producenta, dostawcy usługi lub innego podmiotu odpowiedzialnego za utrzymanie rozwiązania.

6.4. Aktualizacje i obsługa podatności

Zamawiający powinien wiedzieć, w jaki sposób zgłaszane i obsługiwane są istotne podatności dotyczące oferowanego rozwiązania.

Warto określić:

- sposób aktualizacji urządzeń i oprogramowania,
- sposób zgłaszania problemów bezpieczeństwa,
- sposób informowania klientów o istotnych podatnościach,
- odpowiedzialność za aktualizację w okresie wsparcia,
- kanał kontaktu w sprawach bezpieczeństwa produktu lub usługi.

Przykład

Wykonawca przedstawi opis procesu aktualizacji oraz obsługi istotnych podatności dla oferowanych urządzeń, oprogramowania lub usług. Opis może pochodzić od producenta, dostawcy usługi lub innego podmiotu odpowiedzialnego za utrzymanie rozwiązania i powinien wskazywać, w jaki sposób Zamawiający będzie informowany o aktualizacjach bezpieczeństwa, podatnościach oraz zalecanych działaniach utrzymaniowych.

6.5. Integralność firmware i bezpieczna aktualizacja

W przypadku nowych urządzeń telemetrycznych warto zwrócić uwagę nie tylko na możliwość aktualizacji firmware, ale również na sposób zabezpieczenia procesu aktualizacji oraz ochronę przed uruchomieniem nieautoryzowanego lub zmodyfikowanego oprogramowania.

W zależności od klasy urządzenia, funkcji systemu i poziomu ryzyka można wymagać lub premiować:

- mechanizm weryfikacji autentyczności i integralności firmware przed instalacją,
- podpisany firmware lub równoważny mechanizm potwierdzający pochodzenie aktualizacji,
- secure bootloader lub równoważny mechanizm kontroli integralności kodu uruchamianego przez urządzenie,
- zabezpieczenie procesu aktualizacji przed przypadkowym lub nieautoryzowanym wgraniem niewłaściwej wersji firmware,
- możliwość odtworzenia działania urządzenia po nieudanej aktualizacji, jeżeli jest to technicznie uzasadnione,
- dokumentację bezpiecznego procesu aktualizacji.

Wymagania te powinny być stosowane proporcjonalnie do znaczenia urządzenia i funkcji systemu. Inne oczekiwania będą właściwe dla urządzenia

pomiarowego, a inne dla sterownika telemetrycznego, modułu komunikacyjnego lub urządzenia umożliwiającego zdalne sterowanie obiektem.

Informacje dotyczące integralności firmware, podpisywania aktualizacji, secure boot lub równoważnych mechanizmów powinny pochodzić od producenta lub podmiotu odpowiedzialnego za rozwój i utrzymanie firmware, a nie od integratora, który nie ma wpływu na konstrukcję urządzenia.

Przykład

Wykonawca powinien wskazać, czy oferowane urządzenie posiada mechanizmy weryfikacji autentyczności i integralności firmware, podpisany firmware, secure boot, secure bootloader lub równoważne mechanizmy ograniczające ryzyko uruchomienia nieautoryzowanego albo zmodyfikowanego oprogramowania. Informacje te mogą pochodzić z dokumentacji producenta lub od podmiotu odpowiedzialnego za rozwój i utrzymanie firmware.

6.6. Transmisja danych

Jeżeli rozwiązanie wykorzystuje transmisję komórkową lub transmisję przez sieci publiczne, Zamawiający powinien oczekiwać opisu sposobu jej zabezpieczenia.

W zależności od architektury można wymagać lub premiować:

- prywatny APN,
- VPN,
- szyfrowanie transmisji,
- ograniczenie ekspozycji urządzeń i usług do Internetu,
- indywidualne uwierzytelnianie urządzeń, jeżeli ma zastosowanie.

Przykład

Jeżeli oferowane rozwiązanie wykorzystuje transmisję danych przez sieć komórkową lub inną sieć publiczną, Wykonawca opíše sposób zabezpieczenia transmisji. W przypadku transmisji komórkowej Zamawiający może wymagać lub premiować wykorzystanie prywatnego APN, VPN, szyfrowania transmisji oraz ograniczenia ekspozycji urządzeń i usług do Internetu.

6.7. Usługi chmurowe i systemy zdalnego nadzoru

Jeżeli oferowane rozwiązanie obejmuje usługę chmurową, platformę wizualizacji, system alarmowania, raportowania lub zdalnego nadzoru, Zamawiający powinien oczekiwać opisu podstawowych zasad świadczenia i utrzymania usługi.

Warto określić, w szczególności w ramach umowy SLA:

- operatora lub dostawcę usługi,
- lokalizację gromadzenia i przetwarzania danych – Europejski Obszar Gospodarczy,
- podział odpowiedzialności między Zamawiającego, integratora i dostawcę usługi,
- ogólne zasady utrzymania, dostępności i odtwarzania usługi w zakresie udostępnianym klientom,
- zasady zarządzania użytkownikami,
- rejestrowanie istotnych zdarzeń,
- dostępność usługi,
- zasady zakończenia korzystania z usługi i eksportu danych

Przykład

Jeżeli oferowane rozwiązanie obejmuje usługę chmurową lub platformę zdalnego nadzoru, Wykonawca przedstawi opis podziału odpowiedzialno-

ści, lokalizacji gromadzenia i przetwarzania danych, zasad zarządzania użytkownikami, zakresu rejestrowania zdarzeń dostępnych dla Zamawiającego, ogólnych zasad utrzymania i odtwarzania usługi oraz warunków zakończenia korzystania z usługi i eksportu danych, w zakresie wynikającym z umowy, regulaminu lub dokumentacji usługi.

7. Obszary, które warto uwzględnić w ocenie rozwiązania lub dostawcy

Wymagania minimalne zapewniają podstawowy poziom przejrzystości, ale nie zawsze pozwalają wybrać rozwiązanie bardziej dojrzałe i łatwiejsze do utrzymania. Dlatego część elementów warto uwzględnić w ocenie rozwiązania, dostawcy lub modelu utrzymania.

Wagi i sposób oceny powinny być każdorazowo dostosowane do konkretnego postępowania, jego wartości, zakresu, trybu oraz znaczenia systemu dla Zamawiającego.

OBSZAR	CO WARTO OCENIĆ?
Certyfikowany System Zarządzania Bezpieczeństwem Informacji	Czy producent, dostawca usługi lub inny podmiot odpowiedzialny za istotny element rozwiązania posiada certyfikowany SZBI, np. ISO/IEC 27001:2022, w zakresie związanym z oferowanym produktem lub usługą?
Odpowiedzialność w łańcuchu dostaw	Czy wskazano producenta rozwiązania, rolę wykonawcy oraz podmiot odpowiedzialny za rozwój, aktualizacje, dokumentację, obsługę podatności i wsparcie produktu?
Cykl życia i wsparcie produktu	Czy wskazano deklarowany okres wsparcia, zasady aktualizacji, sposób informowania o końcu wsparcia oraz możliwość utrzymania produktu przez lata?
Proces obsługi podatności	Czy producent, dostawca usługi lub podmiot odpowiedzialny za produkt posiada opisany sposób zgłaszania, analizy i komunikowania istotnych podatności dotyczących oferowanego rozwiązania?
Integralność firmware i bezpieczna aktualizacja	Czy producent lub podmiot odpowiedzialny za firmware opisuje mechanizmy weryfikacji autentyczności i integralności firmware, podpisywania aktualizacji, secure bootloader lub równoważne zabezpieczenia procesu uruchamiania i aktualizacji urządzenia?
Bezpieczeństwo transmisji	Czy rozwiązanie przewiduje adekwatne mechanizmy ochrony transmisji, np. prywatny APN, VPN, szyfrowanie transmisji oraz ograniczenie ekspozycji urządzeń i usług do Internetu?
Usługa chmurowa lub zarządzana	Czy opisano podział odpowiedzialności, lokalizację danych, ogólne zasady utrzymania i odtwarzania usługi, zakres rejestrowania zdarzeń dostępnych dla Zamawiającego, dostępność usługi, warunki zakończenia korzystania z usługi i eksportu danych?
Lokalne wsparcie producenta lub autoryzowanej sieci partnerskiej	Czy zapewnione jest wsparcie techniczne w Polsce i w języku polskim, realizowane przez producenta, autoryzowanego dystrybutora, integratora, partnera wdrożeniowego lub inny uzgodniony kanał wsparcia?
Doświadczenie w systemach telemetrycznych dla infrastruktury rozproszonej	Czy dostawca, producent lub integrator posiada doświadczenie w dostawie, wdrażaniu lub utrzymaniu systemów telemetrycznych dla obiektów wod-kan, przemysłowych lub infrastrukturalnych?



8. Certyfikowany System Zarządzania Bezpieczeństwem Informacji

Jednym z elementów, które warto uwzględnić w ocenie rozwiązania lub dostawcy, jest posiadanie certyfikowanego Systemu Zarządzania Bezpieczeństwem Informacji. Nie powinno jednak chodzić o dowolny certyfikat „na firmę”, ale o zakres certyfikacji istotny dla danego projektu lub postępowania.

W zależności od modelu dostawy certyfikat może dotyczyć producenta urządzeń, producenta oprogramowania, dostawcy usługi chmurowej, operatora platformy lub innego podmiotu odpowiedzialnego za istotny element rozwiązania.

Co Zamawiający powinien sprawdzić:

- czy certyfikat jest aktualny,
- kto wydał certyfikat,
- jaki jest zakres certyfikacji,
- czy zakres obejmuje obszary związane z oferowanym rozwiązaniem,
- czy certyfikat dotyczy projektowania, rozwoju, produkcji, sprzedaży, serwisu, utrzymania usług lub przetwarzania danych, zależnie od przedmiotu zamówienia.

Przykład

Zamawiający może premiować posiadanie przez producenta, dostawcę usługi lub inny podmiot odpowiedzialny za istotny element rozwiązania certyfikowanego systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001:2022 lub równoważnego, którego zakres obejmuje czynności związane z oferowanym rozwiązaniem, w szczególności projektowanie, rozwój, produkcję, sprzedaż, serwis urządzeń telemetrycznych, rozwój oprogramowania, utrzymanie usług chmurowych lub przetwarzanie danych telemetrycznych.

9. Kontrola nad produktem, firmware i łańcuchem dostaw

W przypadku urządzeń telemetrycznych istotne jest, czy w łańcuchu dostaw istnieje podmiot posiadający realną kontrolę nad produktem, firmware, aktualizacjami, dokumentacją i obsługą podatności.

Ryzykiem dla Zamawiającego może być zakup rozwiązania, którego oferent jedynie dystrybuje produkt pod własną marką, ale nie jest w stanie wskazać, kto odpowiada za firmware, aktualizacje, podatności, dokumentację techniczną i wsparcie w całym cyklu życia.

Celem wymagań nie powinno być wykluczanie określonych modeli biznesowych, takich jak OEM, tzw. white label, dystrybucja lub integracja. Celem powinno być potwierdzenie, że w łańcuchu dostaw istnieje skuteczny mechanizm utrzymania oferowanego rozwiązania przez deklarowany okres eksploatacji.

Co Zamawiający powinien sprawdzić:

- kto jest rzeczywistym producentem urządzenia,
- kto rozwija i utrzymuje firmware,
- kto przygotowuje aktualizacje bezpieczeństwa,
- kto analizuje i usuwa podatności,
- czy istnieje kanał współpracy z producentem lub podmiotem odpowiedzialnym za produkt,
- czy dostawca, integrator lub dystrybutor posiada dokumentację, upoważnienie, umowę partnerską albo inny mechanizm współpracy umożliwiający skuteczne wsparcie produktu,
- czy występują nieudokumentowane mechanizmy dostępu lub funkcje komunikacyjne.

Przykład

Zamawiający może premiować rozwiązania, w których jasno wskazano producenta, rolę wykonawcy, podmiot odpowiedzialny za firmware, aktualizacje, obsługę podatności, dokumentację techniczną i wsparcie produktu oraz sposób współpracy między tymi podmiotami.

10. Lokalne wsparcie producenta lub autoryzowanej sieci partnerskiej

W przypadku systemów telemetrycznych eksploatowanych przez wiele lat istotne znaczenie ma dostępność wsparcia technicznego, serwisu, konsultacji projektowych oraz kompetencji producenta lub autoryzowanej sieci partnerskiej.

Nie chodzi wyłącznie o lokalizację siedziby dostawcy. Chodzi o praktyczną zdolność do reakcji, zrozumienia lokalnych realiów technicznych i regulacyjnych, wsparcia integratorów oraz pomocy Zamawiającemu w utrzymaniu systemu.

Co Zamawiający powinien sprawdzić:

- czy zapewnione jest wsparcie techniczne w Polsce i w języku polskim,
- czy wsparcie jest realizowane przez producenta, autoryzowanego dystrybutora, integratora, partnera wdrożeniowego lub inny uzgodniony kanał wsparcia,
- czy istnieje jasna ścieżka zgłaszania problemów technicznych, awarii i pytań serwisowych,
- czy dostawca zna realia branży wod-kan,

- czy dostawca, producent lub integrator posiada doświadczenie w infrastrukturze rozproszonej,
- czy istnieje sieć partnerów lub integratorów zdolnych do realizacji wdrożeń i serwisu.

Przykład

Zamawiający może premiować dostępność lokalnego wsparcia technicznego, serwisu, konsultacji projektowych oraz kompetencji producenta lub autoryzowanej sieci partnerskiej, jeżeli mają znaczenie dla utrzymania systemu, czasu reakcji, obsługi awarii, modernizacji lub wsparcia integratora.

11. Własna SCADA a platforma zdalnego nadzoru lub usługa chmurowa

Własny system SCADA daje Zamawiającemu kontrolę nad środowiskiem, ale oznacza również odpowiedzialność za jego aktualizacje, kopie zapasowe, testy odtworzeniowe, przeglądy podatności, konta użytkowników, logi, dokumentację i utrzymanie po zmianie integratora.

Dlatego w projektach telemetrycznych warto pytać nie tylko o funkcje systemu, ale również o to, kto i w jaki sposób będzie odpowiadał za utrzymanie rozwiązania przez kolejne lata.

Jeżeli oferowana jest platforma zdalnego nadzoru, usługa chmurowa lub inna usługa cyfrowa wspierająca telemetrykę, Zamawiający powinien oczekiwać opisu podziału odpowiedzialności oraz zasad świadczenia, utrzymania i zakończenia korzystania z usługi.

Jeżeli dostawca faktycznie realizuje aktywne zarządzanie systemem, urządzeniami, konfiguracją lub środowiskiem technicznym Zamawiającego, zakres takiego zarządzania powinien być opisany odrębnie.

Przykładowe pytania do dostawcy:

- kto odpowiada za aktualizację systemu i komponentów?
- kto odpowiada za kopie zapasowe i odtwarzanie?
- jak rejestrowane są działania użytkowników i administratorów?
- jak wygląda obsługa incydentów i istotnych awarii?
- gdzie są gromadzone i przetwarzane dane?
- jak wygląda zakończenie korzystania z usługi i eksport danych?
- jakie obowiązki pozostają po stronie Zamawiającego?



12. Informacje potrzebne do późniejszego utrzymania systemu lub usługi

Po zakończeniu wdrożenia Zamawiający powinien otrzymać podstawowe informacje umożliwiające eksploatację, serwis, modernizację, odtworzenie lub nadzorowanie systemu w zakresie adekwatnym do rodzaju projektu i modelu dostawy.

Celem nie jest nakładanie nadmiernych obowiązków dokumentacyjnych na dostawcę lub integratora ani wymaganie przekazywania haseł, sekretów technicznych lub dostępu administracyjnego do infrastruktury usługodawcy. Celem jest uniknięcie sytuacji, w której po kilku latach nie wiadomo, jakie rozwiązanie zostało wdrożone, kto odpowiada za jego utrzymanie, jak zgłaszać problemy, jak uzyskać aktualizacje, jak odtworzyć działanie systemu albo jak zakończyć korzystanie z usługi.

Zakres przekazywanych informacji powinien być proporcjonalny do skali wdrożenia oraz zależeć od tego, czy rozwiązanie jest dostarczane jako system wdrożony u Zamawiającego, czy jako usługa chmurowa, platforma zdalnego nadzoru lub model abonamentowy.

System wdrożony u Zamawiającego

Jeżeli rozwiązanie jest wdrażane jako system pozostający w utrzymaniu Zamawiającego lub jego integratora, warto zapewnić, aby Zamawiający posiadał co najmniej:

- listę zastosowanych urządzeń i ich podstawowych wersji oprogramowania,
- informację o producencie urządzeń, oprogramowania lub firmware,
- informację o deklarowanym okresie wsparcia produktu,
- podstawowy opis sposobu komunikacji i transmisji danych,
- informację o sposobie zgłaszania awarii, problemów technicznych i podatności,
- informację o dostępnych aktualizacjach i zasadach ich uzyskania,
- kopię konfiguracji lub informację, w jaki sposób można ją odtworzyć, jeżeli ma to zastosowanie,
- opis znanych ograniczeń rozwiązania, jeżeli mają znaczenie dla utrzymania systemu.

Usługa chmurowa, platforma zdalnego nadzoru lub model abonamentowy

Jeżeli rozwiązanie jest dostarczane jako usługa, Zamawiający nie musi otrzymywać pełnej konfiguracji technicznej zaplecza usługi ani haseł administracyjnych do infrastruktury dostawcy. Powinien natomiast otrzymać informacje pozwalające świadomie nadzorować usługę i korzystać z niej w bezpieczny

sposób, w szczególności:

- wskazanie operatora lub dostawcy usługi,
- opis podziału odpowiedzialności między Zamawiającego, integratora i dostawcę usługi,
- zasady tworzenia, zmiany i odbierania kont użytkowników,
- opis ról i uprawnień dostępnych dla Zamawiającego,
- zasady zgłaszania awarii, incydentów, problemów technicznych i podatności,
- informacje o dostępności usługi i zasadach wsparcia,
- zasady dostępu do danych i ich eksportu.

Przy prostych wdrożeniach wystarczające może być krótkie zestawienie przekazane w dokumentacji powykonawczej, regulaminie usługi lub dokumentacji rozwiązania. Przy większych lub bardziej krytycznych systemach zakres informacji powinien być odpowiednio szerszy.

Przykład

Po zakończeniu wdrożenia Zamawiający powinien otrzymać podstawowe informacje umożliwiające późniejsze utrzymanie systemu albo nadzorowanie świadczonej usługi, w zakresie adekwatnym do przedmiotu zamówienia i modelu dostawy. W przypadku usługi chmurowej, platformy zdalnego nadzoru lub modelu abonamentowego wymagane to nie oznacza obowiązku przekazania haseł administracyjnych ani pełnej konfiguracji infrastruktury dostawcy, lecz obowiązek opisanie zakresu usługi, podziału odpowiedzialności, zasad wsparcia, zarządzania użytkownikami, kopii zapasowych, odtwarzania, dostępu do danych oraz zakończenia korzystania z usługi.

13. Krótka checklista dla Zamawiającego

Przed rozpoczęciem projektu lub ogłoszeniem postępowania warto odpowiedzieć na pytania:

1. Czy kupujemy usługę, dostawę urządzeń, czy wdrożenie rozwiązania obejmującego urządzenia, oprogramowanie i transmisję danych?
2. Czy chcemy jedynie kupić urządzenia, czy także uporządkować utrzymanie systemu?
3. Czy wymagamy wskazania producenta urządzeń, oprogramowania i firmware?
4. Czy wiemy, jaka jest rola wykonawcy w łańcuchu dostaw?
5. Czy wymagamy deklarowanego cyklu życia i wsparcia produktu?
6. Czy chcemy uwzględnić certyfikowany System Zarządzania Bezpieczeństwem Informacji producenta, dostawcy usługi lub innego podmiotu odpowiedzialnego za istotny element rozwiązania?



7. Czy chcemy uwzględnić przejrzystość odpowiedzialności za produkt, firmware, aktualizacje i obsługę podatności?
8. Czy chcemy uwzględnić mechanizmy zabezpieczenia firmware i procesu aktualizacji, takie jak podpisany firmware, secure bootloader lub równoważne mechanizmy?
9. Czy transmisja danych ma być realizowana przez prywatny APN, VPN, szyfrowanie transmisji lub równoważny mechanizm ochrony?
10. Czy rozwiązanie obejmuje usługę chmurową lub platformę zdalnego nadzoru?
11. Czy wiemy, jaki zakres odpowiedzialności zostaje po stronie Zamawiającego?
12. Czy wiemy, jakie informacje są potrzebne do późniejszego utrzymania systemu lub nadzorowania usługi?
13. Czy wymagamy informacji o aktualizacjach i obsłudze podatności?
14. Czy w przypadku systemu wdrożonego u Zamawiającego potrzebne są kopie konfiguracji lub instrukcja ich odtworzenia?
15. Czy w przypadku usługi chmurowej, platformy zdalnego nadzoru lub modelu abonamentowego określono zasady wsparcia, kont użytkowników, kopii zapasowych, odtwarzania i zakończenia korzystania z usługi?
16. Czy sposób oceny ofert premiuje rozwiązania łatwiejsze do utrzymania i bardziej odporne w całym cyklu życia?

14. Podsumowanie

Cyberodporność telemetrii w projektach wod-kan nie powinna polegać na przepisaniu długiej listy technicznych zabezpieczeń. Powinna polegać na

takim ukształtowaniu wymagań, kryteriów oceny i odpowiedzialności dostawców, aby premiować rozwiązania możliwe do bezpiecznego utrzymania przez lata.

W praktyce oznacza to zwrócenie uwagi na dostawcę, producenta, łańcuch dostaw, cykl życia, aktualizacje, obsługę podatności, integralność firmware, bezpieczną aktualizację, transmisję danych, usługi chmurowe, informacje potrzebne do utrzymania systemu, zasady korzystania z usługi i podział odpowiedzialności.

Dobrze przygotowane wymagania pomagają wybrać rozwiązanie, które nie tylko spełnia funkcję techniczną, ale także ogranicza ryzyko organizacyjne, utrzymaniowe i regulacyjne.

Ułatwiają również wykazanie, że decyzja projektowa lub zakupowa była podejmowana świadomie, z uwzględnieniem ryzyka, ciągłości działania i należytej staranności.

Opracowanie: Inventia Sp. z o.o.
© 2026 Inventia Sp. z o.o.
Wszelkie prawa zastrzeżone.

Niniejszy materiał ma charakter informacyjny i pomocniczy. Nie stanowi opinii prawnej, audytu bezpieczeństwa, dokumentacji projektowej ani instrukcji zapewnienia zgodności z regulacjami. Poszczególne wymagania i kryteria należy stosować proporcjonalnie do zakresu projektu, znaczenia obiektów, funkcji systemu, poziomu ryzyka, obowiązujących przepisów oraz decyzji Zamawiającego.



DataPortal platforma zdalnego nadzoru, wizualizacji i alarmowania dla telemetry wod-kan

Współczesna telemetria przestała być wyłącznie narzędziem do zdalnego odczytu danych z obiektów terenowych.

W wielu branżach, a szczególnie w sektorze wodociągowo-kanalizacyjnym, staje się jednym z kluczowych elementów ciągłości działania, zarządzania ryzykiem, dokumentowania zdarzeń oraz zapewnienia cyberodporności infrastruktury technicznej. Przedsiębiorstwa wod-kan zarządzają rozproszonymi obiektami: ujęciami wody, przepompowniami, stacjami uzdatniania, oczyszczalniami, zbiornikami, komorami pomiarowymi, zasuwami i instalacjami terenowymi. Często są to miejsca oddalone, bez stałej obecności obsługi, a jednocześnie istotne dla bezpieczeństwa dostaw wody, ochrony środowiska i sprawnego działania całej sieci.

W takim środowisku znaczenie ma nie tylko samo pozyskanie danych, ale również to, czy informacja dociera szybko, wiarygodnie, w sposób możliwy do odtworzenia i udokumentowania. System telemetryczny powinien więc wspierać nie tylko eksploatację techniczną, ale także zarządzanie, analizę, alarmowanie, raportowanie oraz kontrolę dostępu. Przykładem takiego rozwiązania jest DataPortal – autorski system SCADA zaprojektowany jako zdalny serwis wizualizacji, monitoringu, diagnostyki i zarządzania danymi odebranymi z modułów telemetrycznych.

DataPortal jako alternatywa dla klasycznych systemów SCADA

DataPortal to platforma zdalnego nadzoru i wizualizacji danych telemetrycznych, pełniąca funkcje charakterystyczne dla systemów SCADA w obszarze telemetry. Jego podstawową cechą jest praca w środowisku chmurowym z mechanizmami ochrony dostępu, danych i ciągłości działania. Oznacza to, że użytkownik nie musi budować własnej infrastruktury serwerowej, kupować dodatkowego oprogramowania SCADA/HMI ani utrzymywać specjalistycznego sprzętu pełniącego rolę serwera danych. Do pracy wystarczy dostęp do Internetu, przeglądarka internetowa oraz moduł telemetryczny Inventii z kartą SIM w prywatnym APN.

System umożliwia tworzenie i wyświetlanie animowanych ekranów synoptycznych, gromadzenie danych z urządzeń, ich przetwarzanie, analizę, archiwizację, alarmowanie i raportowanie. Dzięki temu dane pomiarowe nie pozostają jedynie surowymi wartościami liczbowymi, ale są przekształcane w informację przydatną dla operatora, służb utrzymania ruchu, administratora systemu lub kadry zarządzającej. DataPortal pozwala prezentować dane w formie grafik, tabel, wykresów, raportów, zestawień alarmowych i bilansów.

Istotną zaletą tego modelu jest dostępność systemu z różnych urządzeń. Wizualizacja może być urucha-

miana na komputerze, tablecie lub smartfonie, bez konieczności instalowania dodatkowych aplikacji czy wtyczek. System działa przez przeglądarkę internetową, a jego zasoby są dostępne z dowolnego miejsca z dostępem do sieci. W praktyce daje to możliwość szybkiego podglądu pracy obiektu, reakcji na alarmy oraz analizy danych, bez konieczności fizycznej obecności przy lokalnej stacji operatorskiej.

Funkcje systemu DataPortal

DataPortal pełni kilka podstawowych funkcji charakterystycznych dla nowoczesnych systemów SCADA i platform telemetrycznych.

1. Umożliwia zdalny nadzór nad obiektami. Operator może obserwować pracę instalacji, urządzeń i punktów pomiarowych na ekranach synoptycznych.
2. Zapewnia wizualizację danych z modułów telemetrycznych. Dane z obiektów terenowych mogą być przedstawiane w sposób graficzny, czytelny i dostosowany do potrzeb użytkownika.
3. DataPortal obsługuje archiwizację i analizę danych. Dane historyczne mogą być wykorzystywane do oceny pracy obiektu, wykrywania trendów, przygotowywania raportów, analizowania awarii lub rozliczeń.
4. System wspiera alarmowanie i powiadamianie o stanach krytycznych. W przypadku przekroczenia progów alarmowych, zaniku łączności, nieprawidłowej pracy urządzenia lub innego zdefiniowanego zdarzenia, DataPortal może powiadomić odpowiednie osoby. Jest to szcze-

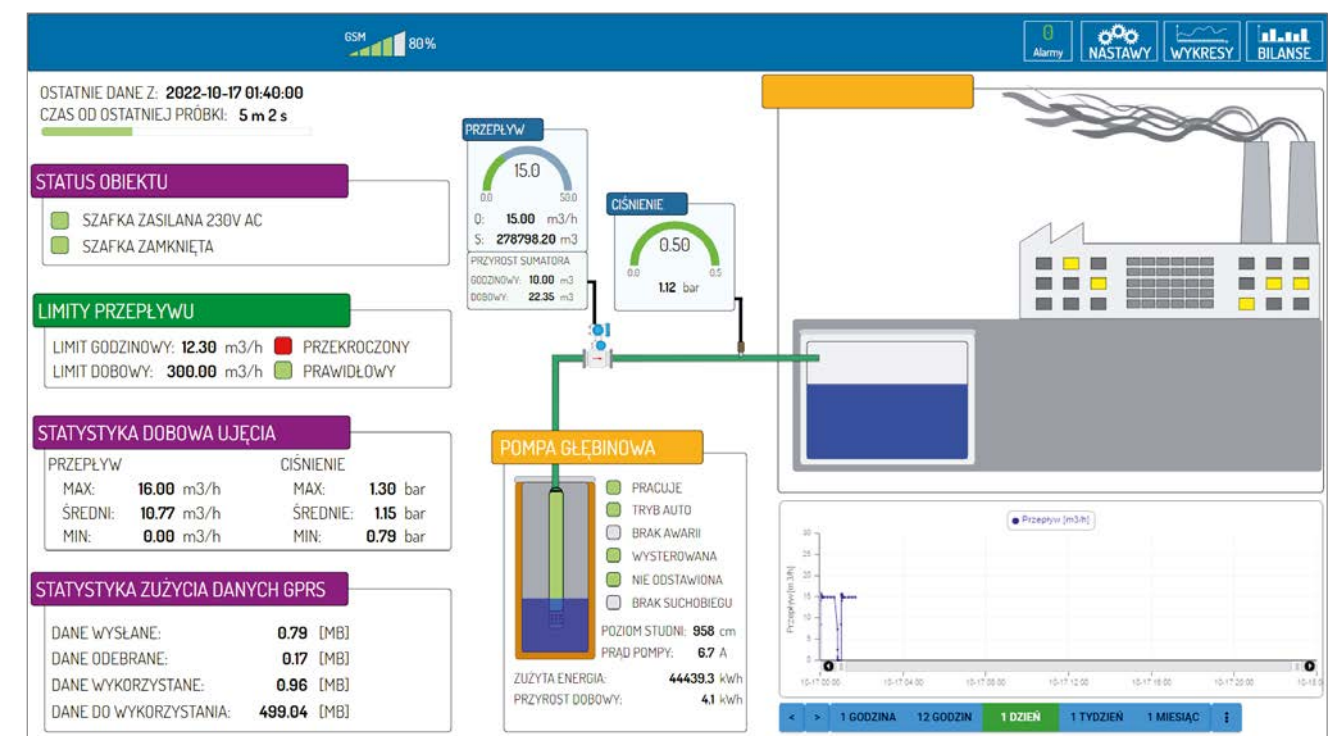
gólnie ważne w przypadku obiektów bez stałej obsługi, gdzie szybkie wykrycie problemu może ograniczyć skutki awarii.

5. DataPortal umożliwia konfigurację wybranych modułów telemetrycznych oraz zarządzanie zasobami, takimi jak urządzenia, źródła danych, tagi, projekty, ekrany, użytkownicy i reguły alarmowe. Oznacza to, że platforma nie jest jedynie pasywnym miejscem prezentacji danych, ale pełni rolę środowiska do zarządzania informacją, wizualizacją i wybranymi elementami infrastruktury telemetrycznej.

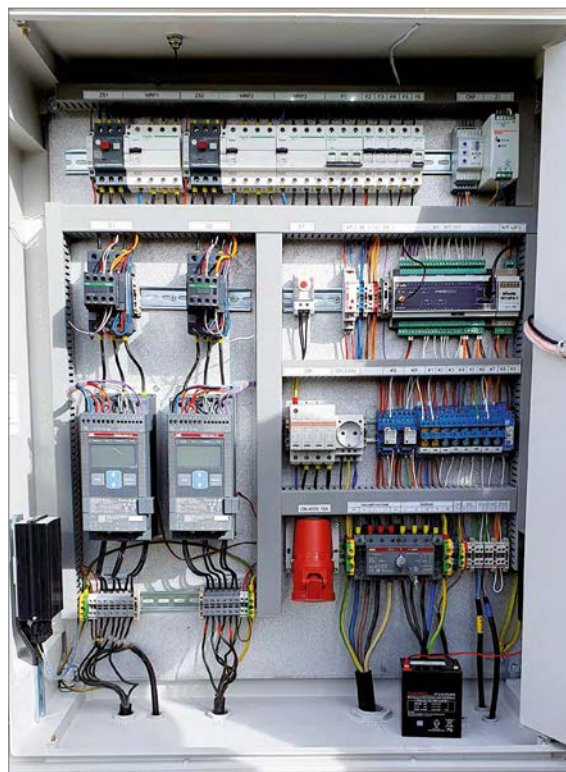
DataPortal w branży wod-kan

Sektor wodociągowo-kanalizacyjny jest naturalnym obszarem zastosowania telemetry. Przepompownie, hydroforne, zbiorniki, komory pomiarowe, stacje uzdatniania i oczyszczalnie są rozproszone geograficznie i często wymagają nadzoru 24/7. Brak informacji z obiektu może oznaczać opóźnioną reakcję na awarię, straty eksploatacyjne, ryzyko środowiskowe lub pogorszenie jakości usług.

DataPortal może wspierać takie przedsiębiorstwa poprzez stałe zbieranie danych, prezentację bieżących parametrów, archiwizację historii pracy, generowanie alarmów i raportów oraz umożliwienie zdalnego wglądu w stan obiektów. Przykładowe zastosowania obejmują monitoring przepływów na cele rozliczeniowe, kontrolę poziomu i ciśnienia, monitoring pracy pomp, obserwację stanów alarmowych, analizę zużycia wody oraz raportowanie parametrów eksploatacyjnych.



W praktyce oznacza to, że system telemetryczny staje się narzędziem nie tylko dla automatyka lub operatora, ale także dla kierownictwa technicznego, działu eksploatacji, utrzymania ruchu i osób odpowiedzialnych za zgodność oraz bezpieczeństwo. Dane z systemu mogą wspierać decyzje operacyjne, analizę reklamacji, ocenę pracy urządzeń, planowanie serwisu oraz dokumentowanie reakcji na zdarzenia.



Cyberodporność telemetry

Pojęcie cyberodporności oznacza zdolność systemu i organizacji do bezpiecznego działania mimo zagrożeń, awarii, incydentów, zmian technologicznych i rosnących wymagań regulacyjnych. W odniesieniu do telemetry nie chodzi wyłącznie o zabezpieczenie hasłem dostępu do systemu. Cyberodporna telemetria obejmuje cały cykl życia rozwiązania: urządzenia, transmisję danych, system nadrzędny, platformę chmurową, aktualizacje, kopie zapasowe, dokumentację, kontrolę dostępu, rejestrowanie zdarzeń, procedury i dostawcę technologii.

W sektorze wod-kan znaczenie cyberodporności rośnie między innymi ze względu na regulację i dobre praktyki związane z cyberbezpieczeństwem, odpornością podmiotów krytycznych, jakością wody, dostępem do usług publicznych oraz normami, takimi jak ISO/IEC 27001 czy IEC 62443. Regulacje te nie wskazują jednego konkretnego systemu, który należy kupić. Zmieniają jednak sposób myślenia o infrastrukturze: ważne staje się to, czy system można

bezpiecznie utrzymywać, aktualizować, dokumentować, audytować i odtwarzać przez cały cykl życia. W tym kontekście DataPortal może być traktowany jako element uporządkowanego ekosystemu telemetrycznego. Platforma zdalnego nadzoru nie zwalnia przedsiębiorstwa z odpowiedzialności za analizę ryzyka, właściwą konfigurację i zarządzanie dostępiami, ale może ograniczać część obowiązków związanych z utrzymaniem własnej infrastruktury serwerowej. Własna SCADA daje dużą kontrolę, ale wymaga samodzielnego dbania o aktualizacje, kopie zapasowe, odtwarzanie, bezpieczeństwo, testy i dokumentację. Model chmurowy może uporządkować część tych obszarów, ponieważ odpowiedzialność techniczna za platformę jest realizowana przez wyspecjalizowanego dostawcę.

Bezpieczeństwo, dostęp i odpowiedzialność

Jedną z ważnych funkcjonalności DataPortalu jest zarządzanie kontami użytkowników i uprawnieniami. System umożliwia rozróżnienie ról, takich jak: administrator, integrator, operator czy obserwator. Każda z tych ról może mieć inny zakres dostępu i odpowiedzialności. Administrator zarządza projektami, źródłami danych, urządzeniami i użytkownikami. Operator może obserwować ekrany i, jeżeli przewidziano taką funkcję, sterować urządzeniami. Obserwator ma dostęp jedynie do podglądu.

Kontrola dostępu ma znaczenie nie tylko organizacyjne, ale również cyberbezpieczeństwa. W systemach telemetrycznych i SCADA należy wiedzieć, kto ma dostęp do danych, urządzeń, funkcji sterujących i konfiguracji. Dostęp powinien być uzasadniony, ograniczony do potrzeb danej roli i możliwy do rozliczenia. W środowisku, w którym systemy są dostępne przez sieć, brak jasnych zasad uprawnień może prowadzić do zwiększenia ryzyka błędów, nadużyć lub trudności w analizie zdarzeń.

DataPortal uwzględnia również kwestie kopii zapasowych, odzyskiwania danych i stabilności systemu. Automatyzacja tworzenia kopii zapasowych oraz mechanizmy przywracania danych po awarii są ważne z punktu widzenia ciągłości działania. W przypadku infrastruktury wod-kan utrata danych lub brak możliwości szybkiego odtworzenia konfiguracji może wydłużyć czas reakcji z godzin do dni. Dlatego kopie zapasowe, dokumentacja i możliwość odtworzenia systemu są elementem cyberodporności, a nie tylko dodatkiem technicznym.

DataPortal – nowa generacja platformy

Nowa wersja DataPortal to technologiczny skok w kierunku poprawy cyberbezpieczeństwa i doposażania platformy do bieżących i nadchodzących regulacji, w pełni oparty o standard ISO/IEC 27001.

Platforma wykorzystuje aktualne wersje technologii, wspiera JSON i REST, a jej architektura została rozdzielona na warstwy: backend, API i frontend. Dzięki temu rozwój systemu, integracje i utrzymanie mogą być prowadzone w sposób bardziej elastyczny.

Istotne znaczenie ma również aspekt cyberbezpieczeństwa. DataPortal wspiera regularne aktualizacje bezpieczeństwa, polityki retencji danych, audyt dostępu oraz logowanie zdarzeń. Są to funkcje ważne z punktu widzenia ochrony danych, kontroli dostępu, zgodności z wymaganiami organizacyjnymi i wykazywania należytej staranności.

Nowy interfejs i wygodniejsza praca

DataPortal wprowadza odświeżony interfejs użytkownika, zachowując znaną logikę pracy z projektami, zasobami, ekranami i raportami. Nowe menu główne oraz drzewo projektowe ułatwiają poruszanie się po systemie i szybszy dostęp do najważniejszych funkcji.

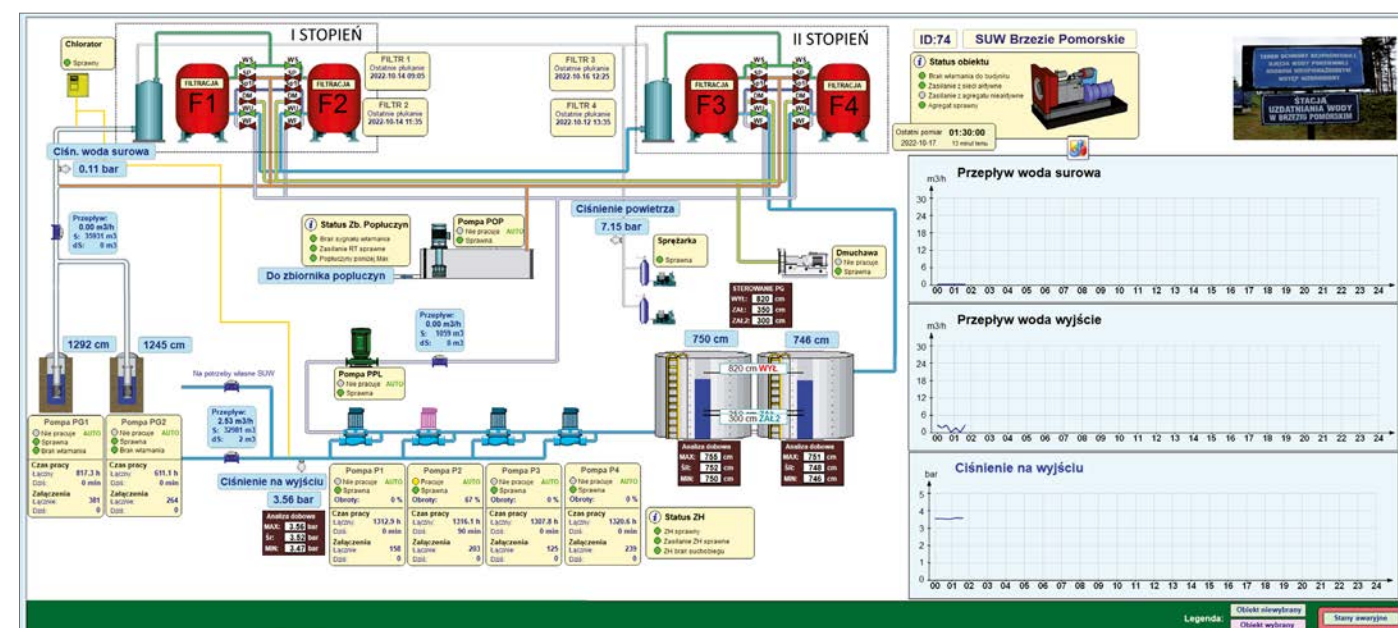
W szczegółach tagów dostępne są ostatnie wartości, historia oraz wykresy z wybranego okresu. Informacje o urządzeniach mogą być uzupełnione zdjęciami modułów telemetrycznych, co pomaga w identyfikacji urządzeń podczas instalacji, serwisu lub inwentaryzacji.

Nowy kreator raportów prowadzi użytkownika przez wybór danych, funkcji agregujących, okresu i formatu raportu. Gotowe raporty można pobierać w formatach m.in. PDF lub Excel.

Alarmy, Designer, komunikaty i pomoc

Obsługa alarmów została uzupełniona o edytor wizualny, który ułatwia przygotowywanie czytelnych komunikatów alarmowych bez konieczności znajomości kodu.

DataPortal Designer zyskał usprawnienia przy projektowaniu ekranów, m.in. wygodniejsze skalowanie, przesuwanie, zarządzanie warstwami oraz



Użytkownik może łatwiej przejść od zarządzania projektem, przez uruchomienie ekranu, aż po jego edycję w DataPortal Designer. Uporządkowane zostały również widoki projektów i ekranów, dodając m.in. szybszy podgląd szczegółów oraz miniatury ekranów.

Zasoby, tagi, urządzenia i raporty

Moduł Zasoby skupia w jednym miejscu tagi, źródła danych, urządzenia i karty SIM. Ułatwia to zarządzanie większymi projektami oraz szybki dostęp do informacji o danych, urządzeniach i ich stanie.

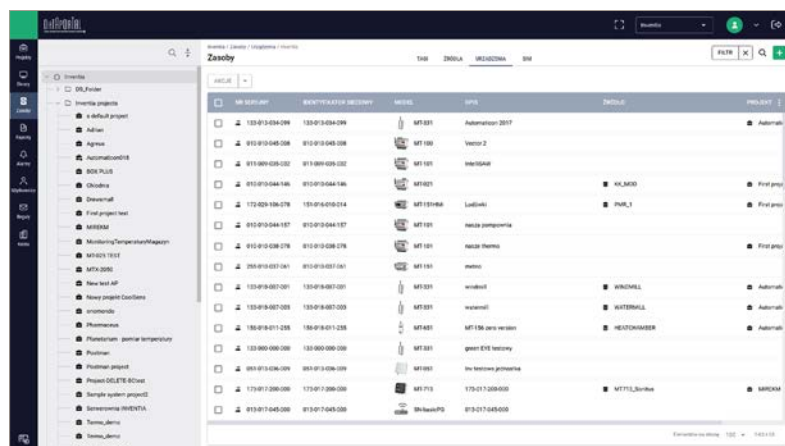
automatyczne nazwy obiektów. Dodano również system komunikatów systemowych oraz nowe Centrum Pomocy online.

Nowe mechanizmy uprawnień i audytowalność

DataPortal wprowadza bardziej szczegółowe zarządzanie uprawnieniami do projektów. Użytkownicy, np. menedżerowie, operatorzy i obserwatorzy, mogą mieć dostęp tylko do wybranych projektów i funkcji.

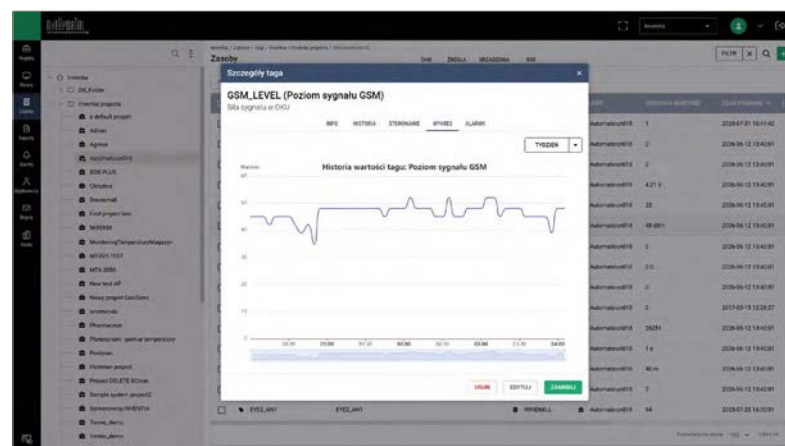
Najważniejsze z punktu widzenia cybersecurity są mechanizmy audytowalności: dziennik zdarzeń

i modyfikacji, historia działań użytkowników, kontrola zmian oraz możliwość analizy aktywności w systemie. Funkcje te wspierają diagnostykę, analizę incydentów, audyt oraz dokumentowanie należytej staranności.



Wizualizacja zakładki Zasoby

Wzmocnione zostało bezpieczeństwo logowania, m.in. przez wymaganie dłuższego hasła. Dzięki temu DataPortal lepiej odpowiada na potrzeby organizacji, które muszą kontrolować dostęp, chronić dane i dokumentować działania w systemach telemetrycznych.



Okno szczegółów taga – wykres

Znaczenie systemu DataPortal dla zarządzania ryzykiem

DataPortal wspiera zarządzanie ryzykiem poprzez porządkowanie zdalnego nadzoru nad infrastrukturą rozproszoną i centralizację informacji potrzebnych do szybkiej reakcji. W przedsiębiorstwach z branży wod-kan ryzyko nie dotyczy wyłącznie awarii pojedynczego obiektu, ale także opóźnionej reakcji, braku wiarygodnych danych, nieczytelnej historii zdarzeń, niekontrolowanego dostępu użytkowników oraz trudności w wykazaniu, co faktycznie wydarzyło się w systemie i jakie działania zostały podjęte.

DataPortal może wspierać ograniczanie tych ryzyk przez zebranie w jednym systemie danych telemetrycznych, wizualizację pracy obiektów, alarmowanie o stanach nietypowych, rejestrowanie istotnych zdarzeń, zarządzanie użytkownikami i rolami oraz narzędzia umożliwiające analizę i raportowanie. Korzystanie z wyspecjalizowanej platformy może również zmniejszyć obciążenie związane z budową i utrzymaniem własnego środowiska serwerowego, co ma szczególne znaczenie dla organizacji, które nie posiadają rozbudowanego zaplecza IT, albo chcą skoncentrować się na eksploatacji infrastruktury wod-kan, a nie na samodzielnym utrzymaniu wszystkich komponentów lokalnego systemu SCADA.

Podsumowanie

DataPortal jest przykładem nowoczesnej platformy, która łączy zdalny nadzór, wizualizację, alarmowanie, raportowanie, archiwizację danych i zarządzanie zasobami w środowisku chmurowym. Jego zastosowanie jest szczególnie uzasadnione w systemach rozproszonych, takich jak infrastruktura wodociągowo-kanalizacyjna, gdzie szybki dostęp do wiarygodnych danych ma bezpośredni wpływ na ciągłość działania, bezpieczeństwo i jakość obsługi.

W kontekście cyberodporności DataPortal należy postrzegać nie tylko jako narzędzie wizualizacji, ale jako element większego ekosystemu zarządzania ryzykiem. Dane, alarmy, historia zdarzeń, kontrola dostępu, kopie zapasowe, dokumentacja, aktualizacje i odpowiedzialny dostawca stają się równie ważne jak same urządzenia telemetryczne.

Najnowsza wersja DataPortal wzmacnia ten kierunek rozwoju. Nowa architektura warstwowa, nowoczesne API, odświeżony interfejs, rozbudowane uprawnienia, dziennik zdarzeń, lepsze raporty, usprawniony Designer, Centrum Pomocy i wbudowane komunikaty systemowe pokazują, że platforma rozwija się w stronę większej przejrzystości, bezpieczeństwa, skalowalności i wygody pracy. Dla przedsiębiorstw wod-kan oznacza to narzędzie, które pomaga **widzieć wcześniej, reagować szybciej i dokumentować lepiej** – a więc realizować podstawowe cele cyberodpornej telemetrii.

Najnowsza wersja DataPortal będzie dostępna jesienią tego roku.



PAKIET 1: Zaawansowany, wielokanałowy monitoring stref i redukcji strat wody

Pozwala na rejestrację przepływów, ciśnień i innych parametrów sieci oraz na komunikację z przepływomierzami elektromagnetycznymi i innymi inteligentnymi urządzeniami (Modbus RTU) w lokalizacjach pozbawionych zasilania sieciowego. Wykonuje pomiary zgodnie z zadanym harmonogramem.

Niezwłocznie informuje o przekroczeniach wartości ostrzegawczych i alarmowych oraz o istotnych zmianach wartości śledzonych parametrów, a także o otwarciu wjazdu do studni czy komory.

Zasilanie bateryjne umożliwia do 10 lat pracy (w zależności od częstości komunikacji i warunków środowiskowych).

Zadania:

- Regularny pomiar oraz informowanie o zmianach i przekroczeniach progów alarmowych i ostrzegawczych ciśnień, poziomu i innych sygnałów analogowych
- Komunikacja z przepływomierzami elektromagnetycznymi oraz innymi urządzeniami
- Obliczanie przepływów chwilowych oraz przepływu całkowitego na podstawie impulsów
- Wykrywanie wejść na teren obiektu

Sprzęt bazowy:

MT-718 – Zaawansowany baterijny moduł rejestrujący z IP68

Baterijny moduł telemetryczny do monitorowania, rejestracji i transmisji danych w sieciach wodociągowych i systemach przemysłowych. Obsługuje 2G/4G/NB-IoT/LTE-M, zapewniając niezawodną komunikację w trudno dostępnych miejscach. Wyposażony w rejestrator (do 65 tys. rekordów), wejścia binarne i analogowe oraz port szeregowy, umożliwia monitoring kluczowych parametrów. Niskie zużycie energii gwarantuje wieloletnią pracę, a obudowa IP68 pozwala na działanie w wymagających warunkach. Wspiera szyfrowaną komunikację.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA
- **DataPortal** – bezpieczny i intuicyjny system wizualizacji w chmurze, niewymagający nakładów na budowę infrastruktury IT

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN telemetria.pl
- **MT-CPV** – inteligentny zasilacz z podtrzymaniem akumulatorowym. Pozwala na podłączenie zewnętrznego źródła zasilania, np. ogniwa fotowoltaicznych
- **Wtyczki oraz przewody sygnałowe** – w wykonaniu ze złączami M12 ułatwiają podłączenie sygnałów do urządzenia
- **Czujniki ciśnienia** – profesjonalne czujniki WIKA, charakteryzujące się niskim zapotrzebowaniem na energię
- **Uchwyty montażowe** – ułatwiają montaż urządzenia na ścianie

PAKIET 2: Zaawansowana automatyka przepompowni ścieków, tłoczni i SUW

Umożliwia zbudowanie rozproszonego systemu sterowania pompowniami, tłoczniami, SUW-ami, zasuwaniami i innymi obiektami terenowymi z dostępnym zasilaniem sieciowym. Samodzielnie steruje pracą obiektów na podstawie zadanych zdalnie nastaw oraz lokalnych pomiarów. Komunikuje się z inteligentnymi urządzeniami za pomocą portów komunikacyjnych i, jeżeli przewiduje to program, przesyła sterowania (np. zmiana częstotliwości wyjściowej falownika).

Na bieżąco raportuje istotne zmiany stanu pracy układu. Niezwłocznie informuje o sytuacjach alarmowych.

Zadania:

- Sterowanie pracą pomp, falowników, zasuwn, zaworów oraz innych elementów wykonawczych
- Monitorowanie kluczowych i dodatkowych parametrów pracy obiektu
- Natychmiastowe zgłaszanie sytuacji alarmowych

Sprzęt bazowy:

MT-151 – Sterownik telemetryczny programowany w środowisku CODESYS®

MT-151 HMI to zaawansowany sterownik PLC z CODESYS®, łączący funkcje monitorowania, sterowania i rejestracji danych. Wyposażony w modem 2G/4G Dual-SIM, zapewnia niezawodną komunikację, a wbudowany wyświetlacz OLED umożliwia lokalny podgląd bez dodatkowego panelu. Obsługuje popularne protokoły (Modbus RTU, Modbus TCP), oferuje zdalną konfigurację i diagnostykę oraz szerokie możliwości integracji i zastosowań w automatyce i infrastrukturze.

Dostępne zasoby I/O można rozbudować przy pomocy ekspanderów. Wspiera szyfrowaną komunikację.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA
- **DataPortal** – bezpieczny i intuicyjny system wizualizacji w chmurze, niewymagający nakładów na budowę infrastruktury IT

Moduły rozszerzeń

- **EX-A8** – dodatkowe 8 wejść analogowych 4-20mA
- **EX-D16** – dodatkowe 8 wejść binarnych i 8 wejść/wyjść binarnych
- **EX-A41** – dodatkowe 4 wejścia i jedno wyjście analogowe 4-20mA

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN telemetria.pl
- **ZA-PWR-HDR-60-24** – zasilacz na szynę DIN o mocy 60 W (wyjście 24V DC/2,5 A)
- **ZA-IO5-151** – symulator wejść i wyjść sterownika, ułatwiający pracę nad programem

PAKIET 3: Centralne bramy komunikacyjne i integracja sieciowa dyspozytorni

Zapewnia skomunikowanie serwera danych lub stacji inżynierskiej z urządzeniami telemetrycznymi rozproszonymi w terenie. Umożliwia wymianę danych pomiędzy obiektami a systemami wyższego rzędu, jak SCADA, czy Historian oraz na zdalne wykonywanie czynności serwisowych, tj. zmiany konfiguracji urządzeń, programowania oraz aktualizacji firmware (FOTA).

Zadania:

- Przekierowywanie ruchu pomiędzy urządzeniami obiektowymi a oprogramowaniem narzędziowym i driverami
- Blokowanie ruchu z nieupoważnionych adresów IP oraz portów

Sprzęt bazowy:

MTX-2050 v4 – 2G/LTE brama komunikacyjna z portem Ethernet

MTX-2050 v4 to zaawansowany router obsługujący transmisję danych w sieciach 2G/3G/LTE oraz komunikację przez Ethernet i porty RS-232/485. Oferuje zarządzanie poprzez WebGUI oraz integrację z systemami automatyki.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN telemetria.pl
- **ZA-PWR-HDR-60-24** – zasilacz na szynę DIN o mocy 60 W (wyjście 24V DC/2,5 A)

ZESTAW KIT DO MODUŁÓW TELEMETRYCZNYCH

Wszystko, czego potrzebujesz do niezawodnej łączności i transmisji danych

NIEZAWODNE POŁĄCZENIE
Stabilna transmisja danych

BEZPIECZNE DANE
Ochrona Twoich modułów

SZYBKA KONFIGURACJA
Szybkie uruchomienie i podłączenie

KOMPATYBILNY
Szeroka zgodność z urządzeniami

PAKIET 4: Podstawowa automatyka mniejszych obiektów wod-kan (lokalne węzły)

Umożliwia tworzenie rozproszonych systemów sterowania obiektów terenowych wyposażonych w zasilanie sieciowe. Sterownik działa autonomicznie, zarządzając pracą obiektów na podstawie zdalnie definiowanych nastaw oraz lokalnych sygnałów pomiarowych.

Zapewnia komunikację z urządzeniami inteligentnymi poprzez dostępne interfejsy, a w zależności od konfiguracji może realizować funkcje sterujące, takie jak np. regulacja częstotliwości falownika. Dostępne zasoby wejść i wyjść pozwalają na obsługę średniej wielkości obiektów.

System na bieżąco monitoruje stan pracy i rejestruje kluczowe zdarzenia, a w przypadku wystąpienia nieprawidłowości natychmiast generuje sygnały alarmowe.

Zadania:

- Sterowanie pracą pomp, falowników, zasuw, zaworów oraz innych elementów wykonawczych
- Monitorowanie kluczowych i dodatkowych parametrów pracy obiektu
- Natychmiastowe zgłaszanie sytuacji alarmowych

Sprzęt bazowy:

MT-121 – Sterownik telemetryczny programowany w środowisku CODESYS®

MT-121 to zaawansowany sterownik PLC z funkcjami telemetrycznymi, łączący programowanie w CODESYS® ze zdalną komunikacją i sterowaniem. Wyposażony w modem GSM 2G/4G z Dual-SIM zapewnia niezawodną transmisję danych. Posiada bogaty zestaw izolowanych wejść i wyjść (binarnych i analogowych), co umożliwia szerokie zastosowanie w automatyce.

Umożliwia zdalną konfigurację, programowanie i diagnostykę OTA, a dzięki obsłudze protokołów Modbus RTU/TCP oraz interfejsom Ethernet i RS-232/485 łatwo integruje się z systemami SCADA i sieciami przemysłowymi.

Dostępne zasoby I/O można rozbudować przy pomocy ekspanderów.

Wspiera szyfrowaną komunikację.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA
- **DataPortal** – bezpieczny i intuicyjny system wizualizacji w chmurze, niewymagający nakładów na budowę infrastruktury IT

Moduły rozszerzeń

- **EX-A8** – dodatkowe 8 wejść analogowych 4-20mA
- **EX-D16** – dodatkowe 8 wejść binarnych i 8 wyjść binarnych
- **EX-A41** – dodatkowe 4 wejścia i jedno wyjście analogowe 4-20mA

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN telemetria.pl
- **ZA-PWR-HDR-60-24** – zasilacz na szynę DIN o mocy 60 W (wyjście 24V DC/2,5 A)
- **ZA-IO5-121** – symulator wejść i wyjść sterownika ułatwiający prace nad programem

PAKIET 5: Ekonomiczny rozproszony monitoring i zdalny odczyt liczników

Pozwala na pomiar dwóch parametrów analogowych, jak: ciśnienie czy poziom wody oraz przepływ. Informuje o przekroczeniach wartości ostrzegawczych i alarmowych.

Niezwłocznie alarmuje o otwarciu włazu do studni czy komory.

Zadania:

- Ciągły pomiar oraz informowanie o zmianach i przekroczeniach progów alarmowych i ostrzegawczych ciśnień, poziomu lub innych sygnałów analogowych
- Obliczanie przepływów chwilowych oraz całkowitego na podstawie impulsów
- Wykrywanie wejść na teren obiektu

Sprzęt bazowy:

MT-025 v3 – Ekonomiczny moduł telemetryczny

MT-025 v3 to kompaktowy moduł telemetryczny przeznaczony do zdalnego monitorowania, sterowania i alarmowania w rozproszonych systemach automatyki. Stanowi ekonomiczne rozwiązanie dla małych instalacji o ograniczonej liczbie sygnałów. Zapewnia transmisję danych w sieciach 2G/4G (w tym LTE Cat M1/NB-IoT).

Posiada interfejsy USB-C i RS-232/485, wbudowany rejestrator danych oraz kompaktową obudowę na szynę DIN, ułatwiającą instalację i eksploatację.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA
- **DataPortal** – bezpieczny i intuicyjny system wizualizacji w chmurze, niewymagający nakładów na budowę infrastruktury IT

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN telemetria.pl
- **ZA-PWR-HDR-60-24** – zasilacz na szynę DIN o mocy 60 W (wyjście 24V DC/2,5 A)



Zapytaj o pakiety
kart SIM

TELEmi

ze stałym IP

prywatny APN telemetria.pl



PAKIET 6: Podstawowy, budżetowy monitoring punktów bez zasilania sieciowego

Umożliwia rejestrację przepływów i ciśnienia w lokalizacjach pozbawionych zasilania sieciowego. Wykonuje pomiary zgodnie z zadaniem harmonogramem. Informuje o przekroczeniach wartości ostrzegawczych i alarmowych. Zasilanie bateryjne pozwala na do 10 lat pracy (w zależności od częstości komunikacji i warunków środowiskowych).

Niezwłocznie informuje o otwarciu włazu do studni czy komory.

Zadania:

- Regularny pomiar oraz informowanie o zmianach i przekroczeniach progów alarmowych i ostrzegawczych ciśnień, poziomu i innych sygnałów analogowych
- Obliczanie przepływów chwilowych oraz przepływu całkowitego na podstawie impulsów
- Wykrywanie wejść na teren obiektu

Sprzęt bazowy:

MT-058 – Zaawansowany baterijny moduł rejestrujący z IP68

MT-058 to baterijny moduł telemetryczny do monitorowania i transmisji danych w miejscach bez zasilania. Dzięki NB-IoT/LTE-M zapewnia energooszczędną komunikację i pracę do 10 lat na baterii. Wyposażony w rejestrator (do 65 tys. rekordów), wejścia binarne/licznikowe i wejście analogowe. Obudowa IP68 pozwala na pracę w trudnych warunkach.

Wspiera szyfrowaną komunikację.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA
- **DataPortal** – bezpieczny i intuicyjny system wizualizacji w chmurze, niewymagający nakładów na budowę infrastruktury IT

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN telemetria.pl
- **MT-CPV** – inteligentny zasilacz z podtrzymaniem akumulatorowym. Pozwala na podłączenie zewnętrznego źródła zasilania, np. ogniw fotowoltaicznych
- **Czujniki ciśnienia** – profesjonalne czujniki WIKA, charakteryzujące się niskim zapotrzebowaniem na energię
- **Uchwyty montażowe** – ułatwiają montaż urządzenia na ścianie

PAKIET 7: Integracja rozproszonych sterowników i inteligentnych urządzeń

Zapewnia skomunikowanie sterowników oraz innych urządzeń firm trzecich wyposażonych w port szeregowy lub Ethernet z obsługą protokołu Modbus. Umożliwia odbieranie danych odczytanych z tych urządzeń oraz przesyłanie do nich sterowań. Pozwala na zdalne wykonywanie czynności serwisowych, tj. zmiany konfiguracji urządzeń, programowanie oraz aktualizacji firmware (FOTA). Niezwłocznie informuje o sytuacjach alarmowych i istotnych zmianach.

Zadania:

- Wzbogacenie istniejących systemów o bezpieczną, zdalną komunikację danych
- Umożliwienie zdalnego dostępu serwisowego
- Blokowanie ruchu z nieupoważnionych adresów IP oraz portów

Sprzęt bazowy:

MT-221 – Brama komunikacyjna programowana w środowisku CODESYS®

MT-221 to nowoczesna brama komunikacyjna integrująca urządzenia pomiarowe, sterowniki PLC i systemy automatyki poprzez sieci 2G/4G, Ethernet oraz RS-232/485. Dzięki środowisku CODESYS® umożliwia elastyczne programowanie i lokalne przetwarzanie danych. Urządzenie może działać jako lokalny Master, cyklicznie zbierając i analizując dane. Technologia Dual-SIM zapewnia niezawodną komunikację, a zdalna konfiguracja i aktualizacja OTA ułatwiają zarządzanie. Wbudowany rejestrator (do 0,1 s) pozwala na zapis i archiwizację danych procesowych.



Dostępne również:

Oprogramowanie

- **MTManager** – darmowe oprogramowanie do lokalnej i zdalnej konfiguracji oraz aktualizacji firmware
- **MTDataProvider** – darmowy driver komunikacyjny, pozwalający w bezpieczny sposób przekazać dane do systemu SCADA
- **DataPortal** – bezpieczny i intuicyjny system wizualizacji w chmurze, niewymagający nakładów na budowę infrastruktury IT

Moduły rozszerzeń

- **EX-A8** – dodatkowe 8 wejść analogowych 4-20mA
- **EX-D16** – dodatkowe 8 wejść binarnych i 8 wejść/wyjść binarnych
- **EX-A41** – dodatkowe 4 wejścia i jedno wyjście analogowe 4-20mA

Akcesoria

- **Zestaw KIT** – antena LTE, kabel USB do lokalnej konfiguracji, pendrive MT-USB z dokumentacją oraz oprogramowaniem
- **TELEmi** – karta SIM ze stałym IP, pracująca w bezpiecznym prywatnym APN'ie telemetria.pl
- **ZA-PWR-HDR-60-24** – zasilacz na szynę DIN o mocy 60 W (wyjście 24V DC/2,5 A)

MT-121 – Sterownik telemetryczny programowany w środowisku CODESYS®

3
LATA
GWARANCJA



8-16DI
/8DO

3AI/1AO

DIN RAIL

RS-232/485

4G



- Programowalny sterownik PLC, bezpłatne środowisko programistyczne CODESYS®
- Wbudowany modem GSM 2G/4G Cat 1
- Technologia Dual-SIM (tryb pasywny) – dostęp do 2 niezależnych sieci GSM zapewnia redundancję infrastruktury transmisyjnej
- 8 wejść binarnych (izolacja galwaniczna)
- 8 wyjść binarnych (możliwość selektywnej konfiguracji jako wejścia, izolacja galwaniczna)
- 3 wejścia analogowe 4–20 mA (izolacja galwaniczna)
- 1 wyjście analogowe 4–20 mA (izolacja galwaniczna)
- Port Ethernet 10Base-T/100Base-TX
- Port szeregowy RS-232/485 dla urządzeń zewnętrznych (izolacja galwaniczna)
- Diagnostyczne diody LED
- Redundantne wejścia zasilające
- Zegar czasu rzeczywistego (RTC)
- Rejestrator danych o rozdzielczości 0,1 s
- Standardowe protokoły komunikacyjne (Modbus RTU, Modbus TCP, przezroczystość)

Sterownik telemetryczny MT-121 przeznaczony jest to realizacji różnych zadań automatyki przemysłowej, procesowej i budynkowej. Posiada środowisko wykonawcze CODESYS, dzięki czemu rozwiązanie łączy w sobie zaawansowane funkcje techniczne i łatwą obsługę. Dodatkowo urządzenie posiada wbudowany rejestrator danych, konwerter protokołów transmisji i bezprzewodowy interfejs komunikacyjny, umożliwiający transmisję danych w sieci 2G/4G. Technologia Dual-SIM zapewnia niezawodność transmisji dzięki dostępowi do dwóch niezależnych sieci 2G/4G.

Przemysłowa konstrukcja, izolacja galwaniczna zasobów, odpowiednio dobrane parametry techniczne oraz łatwe w użyciu narzędzia konfiguracyjne to istotne atuty, dzięki którym MT-121 stanowi optymalne rozwiązanie dla bezprzewodowych systemów telemetrii, nadzoru, diagnostyki i sterowania o podwyższonym poziomie niezawodności. Moduł może być zasilany z dwóch redundantnych źródeł zasilania, o szerokim zakresie napięcia stałego (11–30 V). Wyjście analogowe pozwala na sterowanie w płynny sposób zewnętrznym urządzeniem. Dostępny port Ethernet pozwala na podłączenie rozległej sieci peryferyjnych urządzeń obsługujących Modbus TCP.

Zasoby:

- CODESYS RUNTIME SYSTEM (RTS) z dostępnymi zasobami pamięci 256 kB FLASH, 64 kB RAM
- Tworzenie programu użytkownika przy użyciu bezpłatnego CODESYS Development System zgodnie z IEC 61131-3, z możliwością debugowania
- Integralny, wielozakresowy modem komunikacyjny 2G/4G
- 8 wejść binarnych
- 8 wejść/wyjść binarnych
- 3 wejścia analogowe 4–20 mA (izolacja galwaniczna)
- 1 wyjście 4–20 mA (izolacja galwaniczna)
- Port Ethernet
- 1 port RS-485/RS-232 do dołączania urządzeń zewnętrznych (monitorowanie, diagnostyka)



- Programowa obsługa portu szeregowego FlexSerial
- Zdalna konfiguracja, programowanie, diagnostyka i aktualizacja firmware (OTA)
- Konstrukcja przemysłowa, montaż na szynie DIN, zaciski śrubowe
- 3-letnia gwarancja

- 4 wejścia licznikowe (zamiennie z binarnymi)
- 2 wejścia zasilające
- Wewnętrzna pamięć nieulotna na dane konfiguracyjne z możliwością zdalnej aktualizacji
- Rejestrator pracy urządzenia w pamięci Flash (8 MB)
- Dual-SIM
- Zegar czasu rzeczywistego RTC
- Sygnalizacja pracy LED
- Port USB-C do konfiguracji

Funkcjonalność:

- Tryby komunikacji:
 - » 2G/4G Cat 1 – transmisja danych
 - » SMS
 - » Ethernet
- Dostęp do zasobów wewnętrznych modułu standardowym protokołem Modbus
- Możliwość transmisji danych do/z urządzeń podłączonych do portu komunikacyjnego
- Inteligentny routing pakietów i praca Multimaster w trybie Modbus
- Rosyłanie pakietów w trybie przezroczystym
- Możliwość wykorzystania 4 wejść binarnych jako wejścia licznikowe
- Możliwość samodzielnego zgłaszania zdarzeń alarmowych (unsolicited messages) w wyniku zmiany stanu na wejściu dwustanowym, przekroczenia zadanego progu wartości analogowej lub też spełnienia funkcji logicznej
- Zabezpieczenie przed nieuprawnionym dostępem w postaci listy uprawnionych numerów telefonów i IP, opcjonalnie hasło do konfiguracji
- Możliwość wysyłania SMS w wyniku zaistnienia sytuacji alarmowej, od flagi lub według harmonogramu
- Dynamiczne wstawianie wartości zmiennych w tekst wiadomości SMS
- Rejestrator z rozdzielczością 0,1 sek.

- Programowalne poziomy alarmowe, histereza i stała filtracji dla wejść analogowych
- Możliwość zdalnej zmiany parametrów konfiguracyjnych i programu wewnętrznego modułu
- Przyjazne narzędzia konfiguracyjne
- Łatwa integracja z oprogramowaniem centrum serwisowego
- Diody LED (status modułu, aktywność komunikacji GSM, poziom sygnału GSM, aktywność DATA, aktywność komunikacji szeregowej, stan we/wy binarnych, przekroczenie progu wejścia analogowego, aktywność portu USB, aktywność portu Ethernet, aktywność wejścia zasilania)
- Rozłączalne listwy zaciskowe
- Zasilanie 12V DC / 24V DC
- Montaż na szynie DIN

Ogólne

Wymiary (dł. x szer. x wys.)	105 x 86 x 59 mm
Waga	268 g
Sposób mocowania	Szyna DIN 35mm
Temperatura pracy	-20°C do +55°C
Klasa ochrony	IP20

Modem radiowy

Producent i typ	SIMCom A7672G
Region	globalny
Pasma 2G	850/900/1800/1900 MHz
Pasma 4G	Band: 1, 2, 3, 4, 5, 7, 8, B12, 13, 17, 18, 19, 20, 25, 26, 28, 38, 39, 40, 41, 66
Złącze anteny zewnętrznej	50 Ω, SMA-F

Wejścia binarne I1–I8, IQ1–IQ8

Rodzaj wejść	napięciowe, izolacja galwaniczna
Zakres napięcia zasilania (IQ+ – IQ-)	11 – 30 V
Zakres napięcia wejściowego dla Ix	0 – 30 V
Stan ON (1)	>10 V @ 2,4 mA
Stan OFF (0)	<8 V @ 2,0 mA
Maksymalna częstotliwość impulsów (dla I1 – I4)	250 Hz
Minimalna długość wykrywanego impulsu (dla I1 – I4)	1 ms

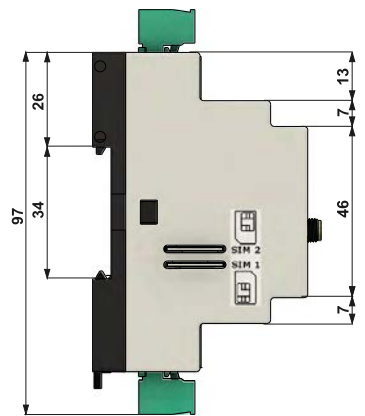
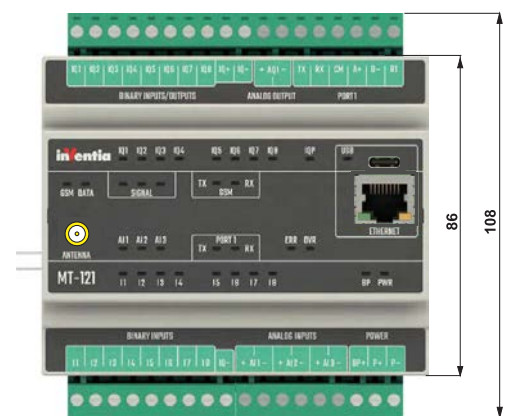
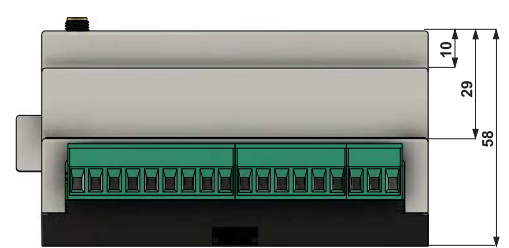
Wyjścia binarne IQ1–IQ8

Rodzaj wyjść	półprzewodnikowe, NO
Zakres napięcia zasilania (IQ+ – IQ-)	11 – 30 V
Maksymalny prąd obciążenia pojedynczego wyjścia	0,2 A
Spadek napięcia na wyjściu (IQ+ – IQx) @0,1 A @0,2 A	0,91 V typ. 1,02 V typ.

Zasilanie

Napięcie stałe DC (nom. 12/24 V)	11 – 30 V DC		
Prąd zasilania (typ.) @ 25°C	Spoczynkowy	Aktywny (Praca)	Maksymalny
12 V DC	0,04 A	0,1 A	1,0 A
24 V DC	0,02 A	0,05 A	0,5 A

Rysunki i wymiary (wszystkie wymiary w milimetrach)



Wejścia analogowe AI1–AI3

Typ wejścia	prądowe, izolacja galwaniczna
Zakres pomiarowy	4 – 20 mA
Maksymalny prąd wejściowy	50 mA
Impedancja dynamiczna wejścia	51 Ω typ.
Rozdzielczość przetwornika A/D	14 bitów
Spadek napięcia dla 20mA	< 5 V
Dokładność wejścia	±0,2 %

Wyjście analogowe AQ1

Rodzaj wyjścia	pasywne (wymagane zewnętrzne zasilanie), izolacja galwaniczna
Zakres wyjścia	4 – 20 mA
Maksymalny prąd wyjścia	50 mA
Zasilanie wyjścia	7,5 – 30 V
Dokładność wyjścia	±0,2 %

MT-121



MT-151 HMI - Sterownik telemetryczny programowany w środowisku CODESYS®

GWARANCJA
3
LATA

CODESYS

PLC

MIM

opcja

SMS

16-28DI
/12DO

6AI

DIN RAIL

RS-232

RS-232/485

4G

DO SPISU TREŚCI

- Programowalny sterownik PLC, bezpłatne środowisko programistyczne CODESYS®
- Wbudowany modem GSM 2G/4G Cat 1
- Technologia Dual-SIM (tryb pasywny) – dostęp do 2 niezależnych sieci GSM zapewnia redundancję infrastruktury transmisyjnej
- 16 wejść binarnych (izolacja galwaniczna)
- 12 wyjść binarnych (możliwość selektywnej konfiguracji jako wejścia, izolacja galwaniczna)
- 4 wejścia analogowe 4–20 mA (izolacja galwaniczna)
- 2 wejścia analogowe 0–10 V (bez izolacji)
- Port Ethernet 10Base-T/100Base-TX
- Port szeregowy RS-232/485 dla urządzeń zewnętrznych (izolacja galwaniczna)
- Port szeregowy RS-232 z zasilaniem 5 V dla paneli operatorskich
- Graficzny wyświetlacz OLED (128x64)
- Diagnostyczne diody LED
- Wejście akumulatora zasilania rezerwowego (wbudowany układ kontroli i ładowania)
- Zegar czasu rzeczywistego (RTC)

* dedykowany firmware

Seria MT-151 to profesjonalne sterowniki telemetryczne najnowszej generacji dla wymagających zastosowań. Model MT-151 HMI v3 LTE łączy funkcje programowalnego sterownika PLC, rejestratora, konwertera protokołów transmisyjnych i bezprzewodowego interfejsu komunikacyjnego, umożliwiającego transmisję danych w sieci 2G/4G. Posiada środowisko wykonawcze CODESYS, dzięki czemu rozwiązanie łączy w sobie zaawansowane funkcje techniczne i łatwą obsługę.

Technologia Dual-SIM zapewnia niezawodność transmisji dzięki dostępowi do dwóch niezależnych sieci 2G/4G różnych operatorów. Port Ethernet otwiera potężne możliwości integracji sterownika z innymi urządzeniami i systemami użytkownika. Wbudowany wyświetlacz OLED z przyciskami do nawigacji ułatwia lokalny podgląd parametrów i wykresów bez konieczności podłączania dodatkowego sprzętu (panel operatorski, komputer przenośny). Przemysłowa konstrukcja, izolacja galwaniczna zasobów, odpowiednio dobrane parametry techniczne oraz łatwe w użyciu narzędzia konfiguracyjne to istotne atuty, dzięki którym urządzenie MT-151 stanowi optymalne rozwiązanie dla bezprzewodowych systemów telemetrycznych, nadzoru, diagnostyki i sterowania o podwyższonym poziomie niezawodności.

Zasoby:

- CODESYS RUNTIME SYSTEM (RTS) z dostępnymi zasobami pamięci 256 kB FLASH, 64 kB RAM
- Tworzenie programu użytkownika przy użyciu bezpłatnego CODESYS Development System zgodnie z IEC 61131-3, z możliwością debugowania
- 16 optoizolowanych wejść binarnych/licznikowych
- 12/24 V DC (I1–I16), logika dodatnia
- 2 wejścia analogowe 0–10 V
- 12 optoizolowanych wyjść binarnych 12/24 V DC (Q1–Q12), logika dodatnia – selektywnie konfigurowalnych jako wejścia



- Rejestrator o rozdzielczości 0,1 s z możliwością zapisu na karcie SD
- Standardowe protokoły komunikacyjne (Modbus RTU, Modbus TCP, IEC 60870-5-104*)
- Tryb FlexSerial dla programowej obsługi protokołów niestandardowych
- Zdalna konfiguracja, programowanie, diagnostyka i aktualizacja firmware (OTA)

- 4 optoizolowane wejścia analogowe 4–20 mA (dokładność 0,2%, 15-bitowa rozdzielczość) z konfigurowaną histerezą i filtracją
- Port Ethernet 10Base-T/100Base-TX
- Izolowany port szeregowy RS-232/485
- Port szeregowy RS-232 z wyjściem zasilania 5 V/500 mA
- Port USB do lokalnej konfiguracji i programowania
- Zaciski zasilania rezerwowego (akumulator SLA 12 V), układ kontroli napięcia i ładowania
- Gniazda dla 2 kart SIM (Dual-SIM)
- Wewnętrzny czujnik temperatury
- Graficzny wyświetlacz OLED i statusowe diody LED
- Wewnętrzne flagi i rejestry dostępne dla użytkownika
- Pamięć Flash na firmware z możliwością zdalnej aktualizacji
- Rejestrator danych i zdarzeń, zapis na karcie SD
- Zegar czasu rzeczywistego RTC (z możliwością zewnętrznej synchronizacji)

Funkcjonalność:

- Tryby komunikacji:
 - » 2G/4G Cat 1 – transmisja pakietowa
 - » SMS
 - » e-mail (bez SSL)
- Dostęp do zasobów modułu standardowym protokołem Modbus RTU, Modbus TCP, Open, Open2
- Inteligentny routing pakietów i praca Multimaster w trybie Modbus
- Rozsyłanie pakietów w trybie przezroczystym
- Praca licznikowa wejść binarnych (do 2 kHz) – I1–I4
- Programowane funkcje logiczne z wykorzystaniem wejść/wyjść, zegarów, liczników, flag i rejestrów w celu wyzwalania zdarzeń (transmisja danych, wysyłanie wiadomości SMS i e-mail, ustawianie wyjść i rejestrów wewnętrznych etc.)

- Transmisja zdarzeniowa w wyniku zmiany stanu wejścia binarnego lub wewnętrznej flagi, przekroczenia zadanego progu wartości analogowej lub spełnienia warunku logicznego
- Wysyłanie wiadomości SMS wyzwalanych zdarzeniami lub według harmonogramu
- Dynamiczne wstawianie wartości zmiennych w polach wiadomości SMS/e-mail
- Konfigurowane progi alarmowe, histereza, przedział nieczułości i stała filtracji dla wejść analogowych
- Transmisja danych z urządzeń zewnętrznych podłączonych do portu RS-232/485
- Napięcie zasilające 5 V dla urządzeń podłączonych do portu RS-232 (np. panel operatorski, odbiornik GPS)
- Możliwość mapowania zasobów urządzeń zewnętrznych w celu wyzwalania zdarzeń
- Zdalna konfiguracja i programowanie przez sieć radiową
- Zabezpieczenia przed nieuprawnionym dostępem – lista autoryzowanych adresów IP i numerów telefonu, opcjonalne hasło, funkcje blokady odczytu konfiguracji
- Montaż na szynie DIN
- Zasilanie 12/24 V DC (24 V DC w przypadku korzystania z akumulatora rezerwowego)
- Kontrola napięcia i ładowania zewnętrznego akumulatora SLA
- Wbudowana autodiagnostyka
- Rozłączalne listwy zaciskowe

Ogólne

Wymiary (dł. x szer. x wys.)	157 x 86 x 58 mm
Waga	382 g
Sposób mocowania	DIN Rail 35 mm
Temperatura pracy	-20 do +65 °C
Wilgotność względna	do 95%, bez kondensacji
Klasa ochrony	IP20

Modem radiowy

Producent i typ	SIMCom A7672G
Region	globalny
Pasma 2G	850/900/1800/1900 MHz
Pasma 4G	Band: 1, 2, 3, 4, 5, 7, 8, B12, 13, 17, 18, 19, 20, 25, 26, 28, 38, 39, 40, 41, 66
Złącze anteny zewnętrznej	50 Ω, SMA-F

Wejścia I1 – I16*

Zakres napięcia wejściowego	0 – 30 V
Prąd wejściowy	2,4 mA
Wejściowe napięcie ON (1)	> 9,4 V
Wejściowe napięcie OFF (0)	< 8,4 V

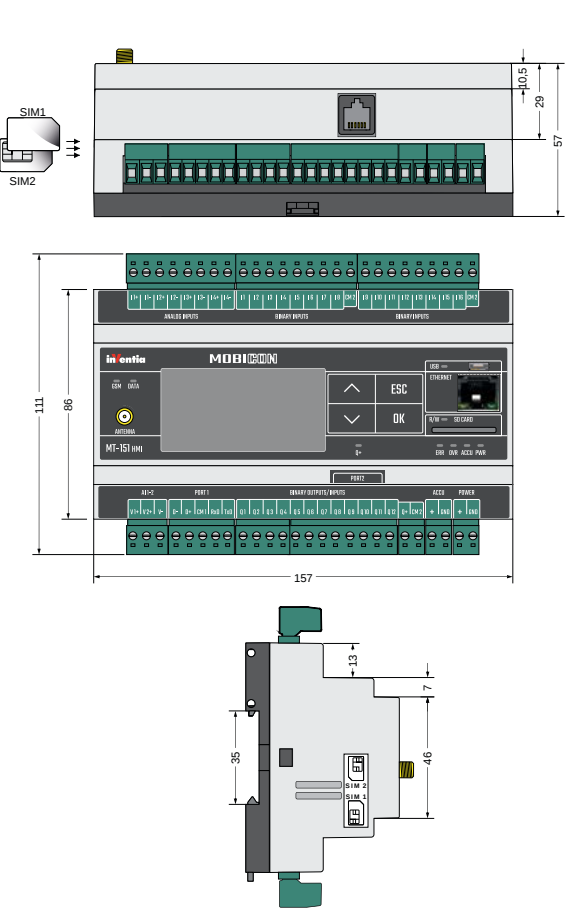
* zgodnie z normą IEC 61131-2

Wejścia Q1 – Q12*

Maksymalne napięcie wyjściowe	30 V
Prąd wyjściowy	2,4 mA
Wejściowe napięcie ON (1)	> 9,4 V
Wejściowe napięcie OFF (0)	< 8,4 V

* zgodnie z normą IEC 61131-2

Rysunki i wymiary (wszystkie wymiary w milimetrach)



Zasilanie

Napięcie stałe (nom. 12/24 V)	10,8 – 30 V		
Prąd wejściowy (@ 24 VDC)	Idle 0,06 A	Active 0,25 A	Max. 1,00 A

Wyjścia Q1 – Q12

Maksymalny prąd wyjściowy	100 mA
Spadek napięcia dla 100 mA	< 0,5 V
Prąd w stanie wyłączonym	< 100 μA

Wejścia analogowe 0 – 10 V (2)

Zakres pomiarowy	0 – 10 V
Maksymalne napięcie wejściowe	20 V
Impedancja wejściowa	197 kΩ typ.
Rozdzielczość przetwornika A/D	16 bitów
Dokładność (@ 25 °C)	0,5 %

Wejścia analogowe 4 – 20 mA (4)

Zakres pomiarowy	4 – 20 mA
Maksymalny prąd wejściowy	50 mA
Impedancja dynamiczna wejścia	55 Ω typ.
Spadek napięcia dla 20mA	< 5 V
Rozdzielczość przetwornika A/D	15 bitów
Dokładność (@ 25 °C)	0,2 %

MT-151 HMI

MT-151 LED - Sterownik telemetryczny programowany w środowisku CODESYS®

GWARANCJA
3
LATA

PLC

opcja

16-28DI
/12DO

6AI

DIN RAIL

RS-232

RS-232/485

4G

DO SPISU TREŚCI

- Programowalny sterownik PLC, bezpłatne środowisko programistyczne CODESYS®
- Wbudowany modem GSM 2G/4G Cat 1
- Technologia Dual-SIM (tryb pasywny) – dostęp do 2 niezależnych sieci GSM zapewnia redundancję infrastruktury transmisyjnej
- 16 wejść binarnych (izolacja galwaniczna)
- 12 wyjść binarnych (możliwość selektywnej konfiguracji jako wejścia, izolacja galwaniczna)
- 4 wejścia analogowe 4–20 mA (izolacja galwaniczna)
- 2 wejścia analogowe 0–10 V (bez izolacji)
- Port Ethernet 10Base-T/100Base-TX
- Port szeregowy RS-232/485 dla urządzeń zewnętrznych (izolacja galwaniczna)
- Port szeregowy RS-232 z zasilaniem 5 V dla paneli operatorskich
- 48 diagnostycznych diod LED
- Wejście akumulatora zasilania rezerwowego (wbudowany układ kontroli i ładowania)
- Zegar czasu rzeczywistego (RTC)

* dedykowany firmware

Seria MT-151 to profesjonalne sterowniki telemetryczne najnowszej generacji dla wymagających zastosowań. Model MT-151 LED v3 LTE łączy funkcje programowalnego sterownika PLC, rejestratora, konwertera protokołów transmisji i bezprzewodowego interfejsu komunikacyjnego, umożliwiającego transmisję danych w sieci 2G/4G. Posiada środowisko wykonawcze CODESYS, dzięki czemu rozwiązanie łączy w sobie zaawansowane funkcje techniczne i łatwą obsługę.

Technologia Dual-SIM zapewnia niezawodność transmisji dzięki dostępowi do dwóch niezależnych sieci 2G/4G różnych operatorów. Port Ethernet otwiera potężne możliwości integracji sterownika z innymi urządzeniami i systemami użytkownika. 48 diagnostycznych diod LED pozwala łatwo określić aktualny stan wejść/wyjść, portów komunikacyjnych i innych zasobów modułu. Przemysłowa konstrukcja, izolacja galwaniczna zasobów, odpowiednio dobrane parametry techniczne oraz łatwe w użyciu narzędzia konfiguracyjne to istotne atuty, dzięki którym urządzenie MT-151 stanowi optymalne rozwiązanie dla bezprzewodowych systemów telemetrycznych, nadzoru, diagnostyki i sterowania o podwyższonym poziomie niezawodności.

Zasoby:

- CODESYS RUNTIME SYSTEM (RTS) z dostępnymi zasobami pamięci 256 kB FLASH, 64 kB RAM
- Tworzenie programu użytkownika przy użyciu bezpłatnego CODESYS Development System zgodnie z IEC 61131-3, z możliwością debugowania
- 16 optoizolowanych wejść binarnych/licznikowych
- 12/24 V DC (I1–I16), logika dodatnia
- 12 optoizolowanych wyjść binarnych 12/24 V DC (Q1–Q12), logika dodatnia – selektywnie konfigurowalnych, jako wejścia
- 4 optoizolowane wejścia analogowe 4–20 mA (dokładność 0,2%, 15-bitowa rozdzielczość) z konfigurowaną histerezą i filtracją
- 2 wejścia analogowe 0–10 V
- Port Ethernet 10Base-T/100Base-TX



- Rejestrator o rozdzielczości 0,1 s z możliwością zapisu na karcie SD
- Standardowe protokoły komunikacyjne (Modbus RTU, Modbus TCP, IEC 60870-5-104*)
- Tryb FlexSerial dla programowej obsługi protokołów niestandardowych
- Zdalna konfiguracja, programowanie, diagnostyka i aktualizacja firmware (OTA)

- Izolowany port szeregowy RS-232/485
- Port szeregowy RS-232 z wyjściem zasilania 5 V/500 mA
- Port USB do lokalnej konfiguracji i programowania
- Zaciski zasilania rezerwowego (akumulator SLA 12 V), układ kontroli napięcia i ładowania
- Gniazda dla 2 kart SIM (redundancja sieci 2G/4G)
- Wewnętrzny czujnik temperatury
- 48 statusowych diod LED (stan wejść/wyjść, zalogowanie do sieci GSM/LTE, aktywna sesja danych, poziom sygnału GSM, aktywność nadawcza i odbiorcza modemu GSM, aktywność nadawcza i odbiorcza portów komunikacyjnych, operacje na karcie SD, status modułu, podstawowe i rezerwowe źródło zasilania)
- Wewnętrzne flagi i rejestry dostępne dla użytkownika
- Pamięć Flash na firmware z możliwością zdalnej aktualizacji
- Rejestrator danych i zdarzeń, zapis na karcie SD
- Zegar czasu rzeczywistego RTC (z możliwością zewnętrznej synchronizacji)

Funkcjonalność:

- Tryby komunikacji:
 - » 2G/4G Cat 1 – transmisja pakietowa
 - » SMS
 - » e-mail (bez SSL)
- Dostęp do zasobów modułu standardowym protokołem Modbus RTU, Modbus TCP, Open, Open2
- Inteligentny routing pakietów i praca Multimaster w trybie Modbus
- Rozsyłanie pakietów w trybie przezroczystym
- Praca licznikowa wejść binarnych (do 2 kHz) – I1–I4
- Programowane funkcje logiczne z wykorzystaniem wejść/wyjść, zegarów, liczników, flag i rejestrów w celu wyzwalania zdarzeń (transmisja danych, wysyłanie wiadomości SMS i e-mail, ustawianie wyjść i rejestrów wewnętrznych etc.)
- Wysyłanie wiadomości SMS wyzwalanych zdarzeniami lub według harmonogramu

- Dynamiczne wstawianie wartości zmiennych w polach wiadomości SMS/e-mail
- Konfigurowane progi alarmowe, histereza, przedział nieczułości i stała filtracji dla wejść analogowych
- Transmisja danych z urządzeń zewnętrznych podłączonych do portu RS-232/485
- Napięcie zasilające 5 V dla urządzeń podłączonych do portu RS-232 (np. panel operatorski, odbiornik GPS)
- Transmisja zdarzeniowa w wyniku zmiany stanu wejścia binarnego lub wewnętrznej flagi, przekroczenia zadanego progu wartości analogowej lub spełnienia warunku logicznego
- Rejestracja danych na karcie SD z rozdzielczością 0,1 s
- Możliwość mapowania zasobów urządzeń zewnętrznych w celu wyzwalania zdarzeń
- Zabezpieczenia przed nieuprawnionym dostępem – lista autoryzowanych adresów IP i numerów telefonu, opcjonalne hasło, funkcje blokady odczytu konfiguracji
- Montaż na szynie DIN
- Zasilanie 12/24 V DC (24 V DC w przypadku korzystania z akumulatora rezerwowego)
- Kontrola napięcia i ładowania zewnętrznego akumulatora SLA
- Wbudowana autodiagnostyka
- Rozłączalne listwy zaciskowe

Ogólne

Wymiary (dł. x szer. x wys.)	157 x 86 x 58 mm
Waga	382 g
Sposób mocowania	DIN Rail 35 mm
Temperatura pracy	-20 do +65 °C
Wilgotność względna	do 95%, bez kondensacji
Klasa ochrony	IP20

Modem radiowy

Producent i typ	SIMCom A7672G
Region	globalny
Pasma 2G	850/900/1800/1900 MHz
Pasma 4G	Band: 1, 2, 3, 4, 5, 7, 8, B12, 13, 17, 18, 19, 20, 25, 26, 28, 38, 39, 40, 41, 66
Złącze anteny zewnętrznej	50 Ω, SMA-F

Wejścia I1 – I16*

Zakres napięcia wejściowego	0 – 30 V
Prąd wejściowy	2,4 mA
Wejściowe napięcie ON (1)	> 9,4 V
Wejściowe napięcie OFF (0)	< 8,4 V

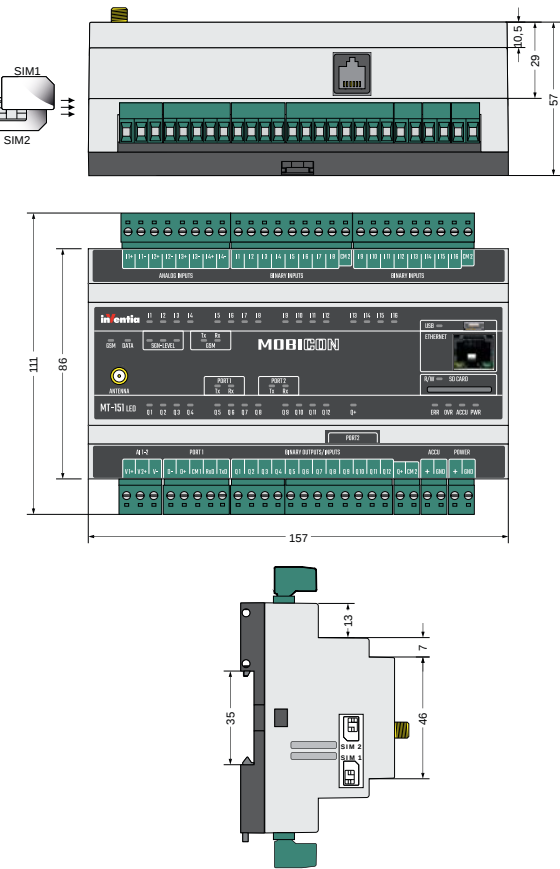
* zgodnie z normą IEC 61131-2

Wejścia Q1 – Q12*

Maksymalne napięcie wyjściowe	30 V
Prąd wyjściowy	2,4 mA
Wejściowe napięcie ON (1)	> 9,4 V
Wejściowe napięcie OFF (0)	< 8,4 V

* zgodnie z normą IEC 61131-2

Rysunki i wymiary (wszystkie wymiary w milimetrach)



Zasilanie

Napięcie stałe (nom. 12/24 V)	10,8 – 30 V		
Prąd wejściowy (@ 24 VDC)	Idle 0,06 A	Active 0,25 A	Max. 1,00 A

Wyjścia Q1 – Q12

Maksymalny prąd wyjściowy	100 mA
Spadek napięcia dla 100 mA	< 0,5 V
Prąd w stanie wyłączonym	< 100 μA

Wejścia analogowe 0 – 10 V (2)

Zakres pomiarowy	0 – 10 V
Maksymalne napięcie wejściowe	20 V
Impedancja wejściowa	197 kΩ typ.
Rozdzielczość przetwornika A/D	16 bitów
Dokładność (@ 25 °C)	0,5 %

Wejścia analogowe 4 – 20 mA (4)

Zakres pomiarowy	4 – 20 mA
Maksymalny prąd wejściowy	50 mA
Impedancja dynamiczna wejścia	55 Ω typ.
Spadek napięcia dla 20mA	< 5 V
Rozdzielczość przetwornika A/D	15 bitów
Dokładność (@ 25 °C)	0,2 %

MT-151 LED

MT-025 v3 – Ekonomiczny moduł telemetryczny

GWARANCJA
3
LATA



4DI/4DO

2AI



DIN RAIL

4G

RS-232/485



- Integralny modem komunikacyjny
- Transmisja pakietowa 2G/4G Cat 1 lub 2G/LTE Cat. M1/NB-IoT
- Opcjonalna obsługa sieci LTE450
- Wejścia binarne/licznikowe (4)
- Wyjścia przekaźnikowe (4)
- Wejścia analogowe (2)
- Gniazdo USB-C do konfiguracji modułu
- Możliwość montażu na szynie DIN
- Konfiguracja przy użyciu komend SMS
- Rejestrator (do 28 000 wpisów)
- Port komunikacyjny RS-232/485 (izolowany)
- Rozłączalne listwy zaciskowe
- 3-letnia gwarancja



Moduł telemetryczny MT-025 v3 to nowa pozycja w segmencie rozwiązań ekonomicznych. Dzięki bardzo atrakcyjnej relacji możliwości do ceny, nowa konstrukcja doskonale nadaje się do zastosowania w systemach zdalnego monitorowania małych, rozproszonych obiektów o niedużej liczbie sygnałów w pojedynczej lokalizacji. Umożliwia zdalne monitorowanie, diagnostykę i sterowanie urządzeniami za pomocą wiadomości tekstowych (SMS) lub/i z wykorzystaniem transmisji pakietowej danych przez sieć operatora LTE. Opcjonalnie przygotowaliśmy MT-025 v3 do pracy z pasmami LTE 450, zapewniając solidną łączność ze zwiększonym zasięgiem i głębszą penetracją sygnału. Konfigurowalne wiadomości tekstowe o stałej lub zmiennej treści (np. zawierające aktualną wartość pomiaru) to wygodny sposób przekazywania informacji do centrum monitoringu lub bezpośrednio pod zdefiniowane numery telefonów pracowników nadzoru. Komunikaty alarmowe mogą być generowane na zmiany stanu wejść binarnych i wyjść binarnych, gdy mierzone wartości analogowe przekroczą próg alarmowy, za pomocą flag timerów i liczników. Komunikacja przez sieć operatora LTE umożliwia bezpieczną i niezawodną komunikację z aplikacjami wyższego rzędu (np. SCADA, bazy danych, systemy oparte na chmurze), pozwalając na rozszerzenie możliwości systemu monitoringu o zdalną komunikację z trudno dostępnymi lub odległymi obiektami.

Moduł MT-025 v3 posiada 4 optoizolowane wejścia binarne, które mogą generować komunikaty alarmowe w celu powiadomienia nadzoru. Wejścia te mogą być skonfigurowane jako wejścia impulsowe. Mogą także współpracować z interfejsem S0 (opcja). Moduł MT-025 v3 wyposażono również w 2 konfigurowalne wejścia analogowe dla pomiaru prądu (4–20 mA) lub napięcia (0–10 V). Dodatkowo, moduł posiada cztery wyjścia przekaźnikowe. Wbudowany rejestrator danych o pojemności 28 000 wpisów umożliwia przechowanie pomiarów w pamięci modułu.

Zastosowania:

- Monitorowanie obiektów
- Systemy alarmowe
- Kontrola dostępu
- Diagnostyka zapobiegawcza

- Zdalny odczyt liczników (AMR)
- Sterowanie przez LTE lub SMS: bramy, pompy, ogrzewanie, oświetlenie etc.

Zasoby:

- Zasilanie (9,5–30 V DC)
- 2 wejścia analogowe nieizolowane 0–10 V/4–20 mA
- 4 wejścia binarne/licznikowe izolowane, logika dodatnia, interfejs S0 (opcja)
- 4 wyjścia przekaźnikowe
- Modem 2G/4G Cat 1 lub 2G/LTE Cat M1/NB-IoT
- Komunikacja MT/SMS
- Złącze konfiguracyjne USB-C
- Zegar czasu rzeczywistego RTC (z możliwością zewnętrznej synchronizacji i podtrzymaniem baterijnym)
- Gniazdo karty SIM
- RS-232/485 izolowany

Funkcjonalność:

- Sposoby komunikacji:
 - » pakietowa transmisja danych
 - » SMS
 - » MQTT 3.1
- Komunikacja zdarzeniowa lub synchroniczna
- Pomiar wartości analogowych:
 - » pomiar napięcia
 - » pomiar prądu
 - » możliwość skalowania wyników pomiarów
 - » definiowanie poziomów alarmowych, filtracji oraz kroku śledzenia dla mierzonych wartości
- Sterowanie wyjściami:
 - » sterowanie bistabilne oraz monostabilne
 - » sterowanie lokalne – sterowanie wyjścia wskutek zaistnienia zdarzenia
 - » sterowanie zdalne – sterowanie wyjścia poprzez zapis wartości do rejestru wyjściowego, SMS
- Timery uniwersalne:
 - » synchronizacja momentu startu zliczania z zegarem RTC

- » konfigurowalny zakres zliczania
- Konfiguracja lokalna i zdalna poprzez komendy SMS oraz dedykowane narzędzia
- Limity transmisji wiadomości SMS
- Dynamiczne wstawianie wartości zmiennych w tekst wiadomości SMS
- Wysyłanie komunikatów SMS do pojedynczych odbiorców lub/i zdefiniowanych grup
- Programowe progi alarmowe, histereza i stała filtracji dla wejść analogowych
- Diody LED (status modułu, aktywność komunikacji, poziom sygnału LTE, stan we/wy binarnych)
- Przyjazne narzędzia konfiguracyjne i diagnostyczne
- Rejestrator danych o pojemności do 28 000 wpisów
- Montaż na szynie DIN

Ogólne

Wymiary (wys. x szer. x głęb.)	70 x 86 x 58 mm
Waga	165 g
Sposób mocowania	DIN Rail 35 mm
Temperatura pracy	-20 do +55 °C
Klasa ochrony	IP20

Modem

Producent / Typ	SIMCom 7672G*	SIMCom SIM7070G*
Region	globalny	globalny
Pasma 2G	850/900/1800/1900 MHz	850, 900, 1800, 1900 MHz
Pasma 4G	B1, B2, B3, B4, B5, B7, B8, B12, B13, B17, B18, B19, B20, B25, B26, B28, B38, B39, B40, B41, B66	B1, B2, B3, B4, B5, B8, B12, B13, B14, B18, B19, B20, B25, B26, B27 (Cat M), B28, B66, B71 (Cat NB), B85
Złącze anteny zewnętrznej	50 Ω, SMA-F	

* zależy od zamówionego wariantu

Zasilanie

Napięcie stałe DC (nom. 12 V / 24 V)	9,5–30 V		
Prąd zasilania, (typ.) @ 25°C	Spoczynkowy	Aktywny (Praca)	Maksymalny
12 V DC	0,01 A	0,2 A	1,0 A
24 V DC	0,005 A	0,1 A	0,5 A

Wejścia binarne I1 – I4*

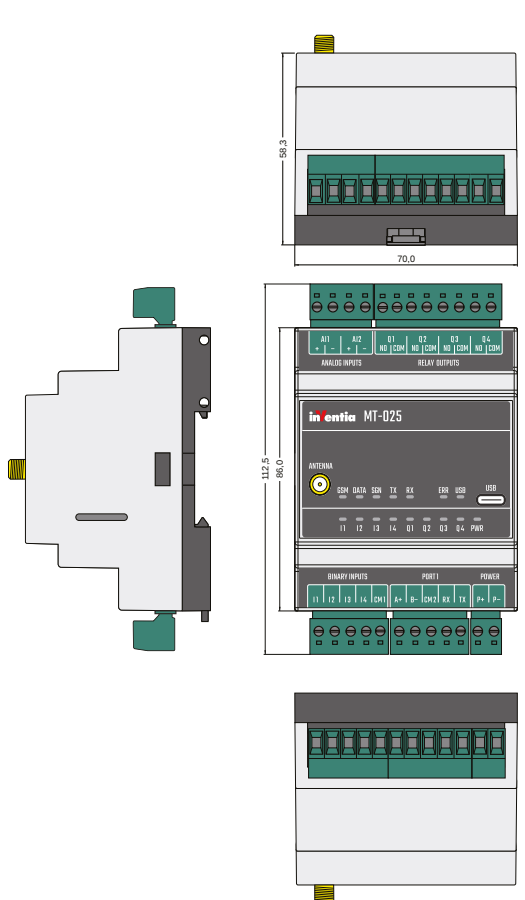
Rodzaj wejść	napięciowe, optoizolowane
Zakres napięcia wejściowego	0–30 V
Stan ON (1)	>9 V @ 1,5 mA
Stan OFF (0)	<3 V @ 0,4 mA
Maksymalna częstotliwość impulsów	250 Hz
Minimalna długość wykrywanego impulsu	2 ms

* opcja – możliwość podłączenia interfejsu S0

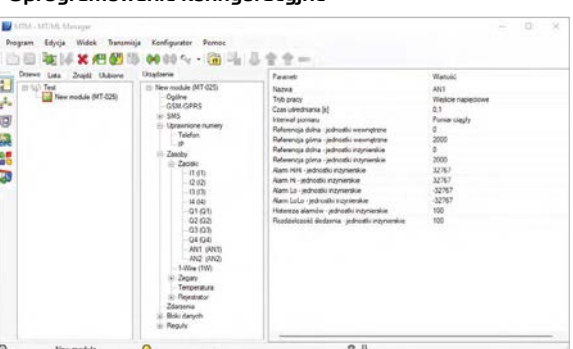
Wyjścia binarne Q1 – Q4

Rodzaj wejść	Przekaźnikowe, izolowane, NO
Maksymalne napięcie styków	250 V AC/30 V DC
Maksymalny prąd styków	5 A (obciążenie rezystancyjne) 2 A (obciążenie indukcyjne)
Rezystancja zestyków	< 100 mΩ

Rysunki i wymiary (wszystkie wymiary w milimetrach)



Oprogramowanie konfiguracyjne



Wejścia analogowe AN1, AN2 – pomiar napięcia

Zakres pomiarowy	0–10 V
Maksymalne napięcie wejściowe	12 V
Rezystancja wejściowa	213 kΩ typ.
Dokładność	±1,5 % max.
Nieliniowość	±1 % max.

Wejścia analogowe AN1, AN2 – pomiar prądu

Zakres pomiarowy	4–20 mA
Maksymalny prąd wejściowy	40 mA
Rezystancja wejściowa	340 Ω typ.
Spadek napięcia dla 20 mA	6,9 V
Dokładność	±1,5 % max.
Nieliniowość	±1 % max.

MT-025 v3

MT-718 PS – bateryjny, energooszczędny moduł rejestrujący z IP68

3
LATA

energy efficient

MIM
opcja

SMS

GPS
opcja

OLED
opcja

5DI / 2DO

2AI

IP68

RS-485
MODBUS . RTU

4G

opcja

DO SPISU TREŚCI

- Transmisja pakietowa 2G/4G Cat 1 lub 2G/NB-IoT/LTE Cat. M1 zależnie od zamontowanego modemu
- 5 wejść dwustanowych/licznikowych z możliwością podłączenia zestyków beznapięciowych (np. wyjść impulsowych przepływomierzy)
- 2 wejścia analogowe 0–5 V DC z konfigurowanymi progami alarmowymi i histerezą, możliwość konwersji do dwóch sygnałów wejściowych 4–20 mA na 0–5 V DC
- 2 wyjścia sterujące
- Kluczowane źródło napięcia 0–5 V DC dla zewnętrznych przetworników analogowych
- Standardowe źródło napięcia 15/24 V DC dla zewnętrznych przetworników
- Czujnik otwarcia obudowy
- Wbudowany przetwornik ciśnienia 0-10 bar (opcjonalnie inne zakresy)
- Opcjonalny cyfrowy czujnik wilgotności wewnątrz obudowy
- Wbudowany czujnik temperatury
- Inteligentny rejestrator danych (8/16* MB pamięci Flash, 30/65* tyś. rekordów, min. interwał zapisu 1 s)
- Konfigurowane harmonogramy i zdarzenia inicjujące pomiary i transmisję danych
- Zegar czasu rzeczywistego RTC
- Wymienne wewnętrzne zasilanie bateryjne (baterie alkaliczne lub litowe)
- Dodatkowe wejście zasilania zewnętrznego 3–8 V DC
- Opcjonalne zasilanie zewnętrzne (MT-CPV)
- uProg – skrypt rozszerzający funkcjonalność modułu
- Wbudowane algorytmy: regulacja zaworu PRV, obsługa sondy Geonor M-600, zmienne alarmy godzinowe
- Inteligentne zarządzanie energią
- Czujnik zużycia ładunku pakietu bateryjnego
- Opcjonalny, wbudowany wyświetlacz OLED
- Port USB-C do lokalnej konfiguracji

* opcja

MT-718 PS to wersja bateryjnego modułu pomiarowego, rejestrującego i transmisyjnego. Podobnie jak inne moduły z rodziny MT charakteryzuje się nowatorskimi rozwiązaniami, łatwością samodzielnego konfigurowania i integrowania z systemami gromadzenia i przetwarzania danych. Możliwości inicjowanego przez moduł przekazu danych (tzw. transmisja spontaniczna lub zdarzeniowa) pozwalają zminimalizować koszty transmisji i zużycia energii, przyczyniając się do wydłużenia czasu pracy na bateriach. Prosta, zwarta, wodoszczelna konstrukcja z elektroniką zabezpieczoną przed wpływem wilgoci, umożliwi bezpośrednią instalację modułu w trudnych warunkach środowiskowych, w miejscach pozabawionych zasilania zewnętrznego (np. w komorach pomiarowych sieci wodociągowej). Moduł możemy zasilac z zestawu baterii możliwego do wymiany przez Użytkownika lub z zewnętrznego pakietu bateryjnego poprzez dodatkowy moduł MT-CPV. Poziom napięcia baterii jest stale monitorowany i przekazywany wraz z danymi pomiarowymi. Moduł MT-718 PS wyposażony jest w 5 wejść dwustanowych/licznikowych (przystosowanych do współpracy ze stykiem beznapięciowym, np. impulsatora wodomierza) oraz 2 wejścia analogowe, umożliwiające pomiar takich parametrów jak: ciśnienie, temperatura, poziom oraz wbudowany przetwornik ciśnienia z szybkozłączem, zapewniającym wygodne połączenie z elastycznym przewodem ciśnieniowym. Dodatkowo



- Interfejs RS-485 z obsługą protokołu Modbus RTU
- Opcjonalny interfejs BLE
- Wodoszczelna obudowa zabezpieczająca przed wpływem wilgoci
- Obsługa komunikacji z zewnętrznym odbiornikiem GPS (dedykowane wyjście zasilania 5 V DC, obsługiwane odbiorniki z interfejsem CMOS TTL i RS-485 oraz protokołem NMEA)
- Dostępne obudowy w wariacie z dławnicami lub złączami M12
- Zewnętrzne gniazdo antenowe typu SMA
- Przyjazne oprogramowanie konfiguracyjne i komunikacyjne
- Oprogramowanie do zdalnego zarządzania poprzez transmisję pakietową i BLE
- Wbudowana karta MIM (opcja) – dostęp do 2 niezależnych sieci GSM zapewnia redundancję infrastruktury transmisyjnej
- Zdalna aktualizacja oprogramowania

istnieje możliwość wykorzystania wbudowanego konwertera 2 sygnałów analogowych 4–20 mA, na sygnał napięciowy 0–5 V. Moduł posiada również interfejs RS-485 obsługujący między innymi protokół Modbus RTU oraz NMEA umożliwiający podłączenie zewnętrznych urządzeń, w tym również odbiornika GPS.

Niezwykle niskie zużycie energii uzyskano m.in. dzięki kluczowaniu źródła zasilającego wejścia analogowego i źródła zasilającego urządzenia zewnętrzne tylko na czas pomiaru oraz dzięki zaawansowanym trybom pracy wbudowanego modemu komunikacyjnego. Dane pomiarowe mogą być rejestrowane z precyzyjnym stemplem czasowym w nieulotnej pamięci Flash, zgodnie z harmonogramem czasowym lub zdarzeniowo. Opcjonalnie dane pomiarowe można zaprezentować na ekranach wbudowanego wyświetlacza OLED.

Poza funkcjami pomiarowymi moduł może także zgłaszać stany alarmowe, jak np.: otwarcie obudowy, nieautoryzowane otwarcie komory, długookresowy brak przepływu, przekroczenie zadanego poziomu, czy przekroczenie zadanej temperatury. Zasoby i funkcjonalność modułu MT-718 PS mogą być optymalizowane dla konkretnych zastosowań, dzięki wielu opcjom: baterie litowe, złącza M12, wbudowany wyświetlacz OLED, wersja z modemem 2G/4G Cat M1/4G Cat NB1, moduł BLE.

Ogólne

Wymiary (dł. x szer. x wys.)	203 x 125 x 90 mm
Waga (z bateriami)	1,83 kg
Sposób mocowania	4 otwory Ø4, 127x108 mm
Temperatura pracy (baterie alkaliczne)	-20 do +55 °C
Temperatura pracy (baterie litowe)	-30 do +65 °C
Klasa ochrony	IP 68: 2m przez 24h (dla M12 4m przez 30 dni)*
Materiał wykonania obudowy	poliwęglan (UL94V-0)

* bez przepustu wentylacyjnego

Modem

Producent / Typ	SIMCom 7672G*	SIMCom SIM7070G*
Region	globalny	globalny
Pasma 2G	850/900/1800/1900 MHz	850, 900, 1800, 1900 MHz
Pasma 4G	B1, B2, B3, B4, B5, B7, B8, B12, B13, B17, B18, B19, B20, B25, B26, B28, B38, B39, B40, B41, B66	B1, B2, B3, B4, B5, B8, B12, B13, B14, B18, B19, B20, B25, B26, B27 (Cat M), B28, B66, B71 (Cat NB), B85
Złącze anteny zewnętrznej	50 Ω, SMA-F	

* zależy od zamówionego wariantu

Zasilanie

Zestaw baterii wewnętrznych: - 6 baterii alkalicznych lub - 6 baterii litowych	4,5 V/32 Ah 3,6 V/78 Ah
Napięcie zasilania zewnętrznego	3,0 – 8,0 V
Maksymalny prąd w impulsie	< 3 A
Średni prąd w stanie uśpienia modemu	< 250 uA

Wejścia analogowe AN1–AN2 (napięciowe, różnicowe)

Zakres pomiarowy	0 – 5 V
Rezystancja wejściowa	>600 kΩ typ.
Rozdzielczość	12 bitów
Dokładność	± 0,5 %

Wejścia binarne/licznikowe I1–I5

Polaryzacja styków zwrotnych	3 V
Częstotliwość zliczania	250 Hz max.
Minimalna długość impulsu	2 ms

Wbudowany przetwornik ciśnienia AN3

Zakres pomiarowy	0 – 10 bar
Temperatura medium	0 – 80 °C
Dokładność	0,5 %

Wyjścia NMOS Q1, Q2

Napięcie maksymalne	30 V
Prąd maksymalny	250 mA
Prąd wyłączenia	<50 μA
Rezystancja	1 Ω

Konfigurowalne wyjście napięciowe Vo

Zakres napięć	0,0 – 5,0 V
Rozdzielczość	0,1 V
Dokładność	2%
Prąd maksymalny	100 mA

Wyjście napięciowe Vh

Napięcie wyjściowe	15 V lub 24 V
Dokładność	5 %
Prąd maksymalny	50 mA

Wyjście napięciowe Vs

Napięcie wyjściowe	5,0 ± 0,1 V
Prąd maksymalny	100 mA

Rejestrator

Typ pamięci	FLASH
Pojemność pamięci	8 / 16 MB (opcja)
Minimalny okres zapisu	1 s
Liczba rekordów	30 tys. / 60 tys. (opcja)

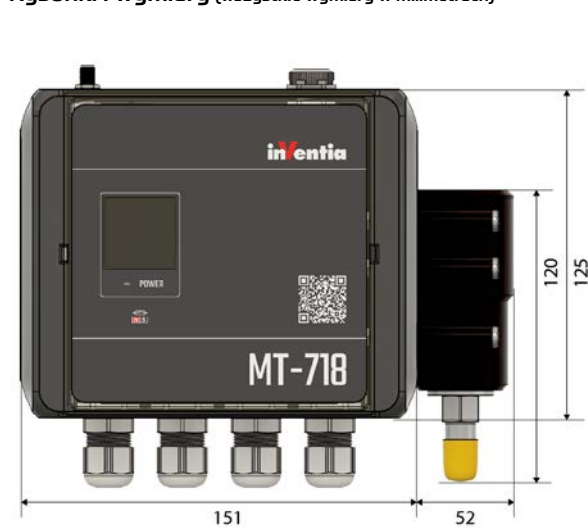
Wyświetlacz OLED (opcja)

Technologia	OLED RGB
Wielkość (przekątna)	1,5"
Rozdzielczość	128 x 128

Interfejs szeregowy

Typ	RS-485
Prędkość transmisji	1200 - 9600 bps
Protokół	MODBUS RTU Master
Liczba obsługiwanych bloków danych	16

Rysunki i wymiary (wszystkie wymiary w milimetrach)



MT-718 PS

MT-058 – bateryjny moduł telemetryczny z IP68

- Integralny modem NB-IoT/LTE Cat. M1
- Pakietowa transmisja danych
- Opcja wlotowej karty MIM zastępującej kartę SIM
- Złącze SMA do zewnętrznej anteny GSM
- Obudowa IP68: 2 m przez 24h
- 5 wejść dwustanowych/2 wejścia licznikowe
- Diagnostyczne diody LED
- Wbudowany pakiet baterijny
- Inteligentne zarządzanie energią
- Rejestrator danych
- Zdalna konfiguracja, aktualizacja i diagnostyka
- Port USB-C do lokalnej konfiguracji
- Do 5 lat pracy na baterii wewnętrznej (do 10 lat na opcjonalnej baterii litowej)
- Port 1-wire dla zewnętrznego czujnika temperatury
- Obsługa MQTT z pełnym wsparciem szyfrowania SSL
- Elektronika pokryta powłoką ochronną, zwiększającą odporność na wilgoć, pył i czynniki środowiskowe



MT-058 to nowoczesny, baterijny moduł telemetryczny zaprojektowany z myślą o niezawodnym monitoringu rozproszonych obiektów infrastrukturalnych. Dzięki obsłudze energooszczędnych technologii LTE Cat. M1 oraz NB-IoT urządzenie zapewnia wyjątkowo niski pobór energii, umożliwiając wieloletnią pracę bez konieczności wymiany baterii. W zależności od konfiguracji i warunków eksploatacji czas autonomicznej pracy może sięgać nawet 10 lat.

Moduł został wyposażony w kompaktową, szczelną obudowę o klasie ochrony IP68 oraz elektronikę pokrytą specjalną powłoką ochronną, która zwiększa odporność na wilgoć, pył i niekorzystne warunki środowiskowe. Dzięki temu MT-058 doskonale sprawdza się w aplikacjach wodociagowych, ciepłowniczych, energetycznych i środowiskowych, także w miejscach pozbawionych dostępu do zasilania sieciowego.

Elastyczna architektura wejść i interfejsów pozwala na współpracę z wodomierzami, przepływomierzami, czujnikami ciśnienia, temperatury oraz sygnałami alarmowymi. Wbudowany rejestrator danych gwarantuje zachowanie pomiarów nawet podczas czasowej utraty łączności, a transmisja cykliczna lub zdarzeniowa umożliwia optymalne dopasowanie pracy urządzenia do wymagań aplikacji.

MT-058 może być zasilany zarówno z baterii, jak i z zewnętrznych źródeł energii, takich jak akumulator współpracujący z panelem fotowoltaicznym. Inteligentne zarządzanie zasilaniem automatycznie przełącza źródło energii, zapewniając ciągłość działania systemu.

Urządzenie obsługuje nowoczesne protokoły komunikacyjne, w tym MQTT z pełnym wsparciem szyfrowania SSL, co umożliwia bezpieczną integrację z platformami IoT, systemami SCADA oraz rozwiązaniami chmurowymi. Dodatkowo dostępna jest możliwość zastosowania przemysłowej karty MIM, montowanej bezpośrednio na płycie urządzenia, zwiększającej niezawodność komunikacji w wymagających warunkach eksploatacyjnych.

Funkcjonalność

- LTE-M / NB-IoT – energooszczędna transmisja danych
- MQTT z pełnym wsparciem szyfrowania SSL
- Możliwość rozbudowy zasobów I/O za pomocą płytki rozszerzeń:
 - 4 dodatkowe wejścia binarne
 - 2 dodatkowe wejścia analogowe 0–5 V
 - 2 dodatkowe wejścia PT1000
- Automatyczne zgłaszanie zdarzeń alarmowych (unsolicited messages)
- Programowalne progi alarmowe, histereza oraz filtracja sygnałów analogowych
- Wbudowany rejestrator danych o rozdzielczości 1 s
- Zdalna zmiana parametrów konfiguracyjnych

Bezpieczeństwo

- Lista dozwolonych adresów IP
- Ochrona konfiguracji hasłem
- Szyfrowana komunikacja MQTT (SSL)

Obsługa i diagnostyka

- Przyjazne narzędzia konfiguracyjne
- Diody diagnostyczne LED

Konstrukcja

- Rozłączalne listwy zaciskowe
- Elektronika pokryta powłoką ochronną zwiększającą odporność na wilgoć, pył i czynniki środowiskowe
- Stopień ochrony IP68

Ogólne

Wymiary (dł. x szer. x wys.)	151 x 80 x 60 mm
Sposób mocowania	4 otwory, 63x127 mm
Temperatura pracy	-20 do +60 °C
Klasa ochrony	IP 68: 2m przez 24h
Materiał wykonania obudowy	poliwęglan (UL94V-0)

Modem

Typ modemu	Nordic nRF9160
Pasma modemu	
LTE Cat-M1:	B1, B2, B3, B4, B5, B8, B12, B13, B14, B18, B19, B20, B25, B26, B28, B66
Cat-NB1/NB2:	B1, B2, B3, B4, B5, B8, B12, B13, B17, B19, B20, B25, B26, B28, B66
Antena	50 Ω

Zasilanie wewnętrzne

Pakiet baterii alkalicznych 4,5 V	7,8 Ah	czas pracy do 5 lat
Pakiet baterii litowych 3,6 V	13 Ah	czas pracy do 10 lat

Zasilanie zewnętrzne

Zakres napięcia zasilania	7–24 V DC
Maksymalny pobór prądu	0,3 A

Wejścia binarne I1–I5

Polaryzacja styków zwiernych	3,3 V
Częstotliwość zliczania (wypełnienie 50%), tylko I1–I2	250 Hz max.
Minimalna długość impulsu – praca jako wejście impulsowe, tylko I1–I2	2 ms
Minimalna długość impulsu – praca jako wejście binarne, tylko I1–I2	2 ms

Wejścia analogowe AI1 (z zasilaniem 5 V DC)

Zakres pomiarowy	0–5 V DC
Rozdzielczość	12 bitów
Dokładność	± 0,5 %

Rejestrator

Typ pamięci	FLASH
Maksymalna liczba rekordów	20 480
Maksymalna liczba rekordów MQTT	2 048

Port 1-wire

Kompatybilny z czujnikiem temperatury	DS18B20
Napięcie zasilania	3,3 V

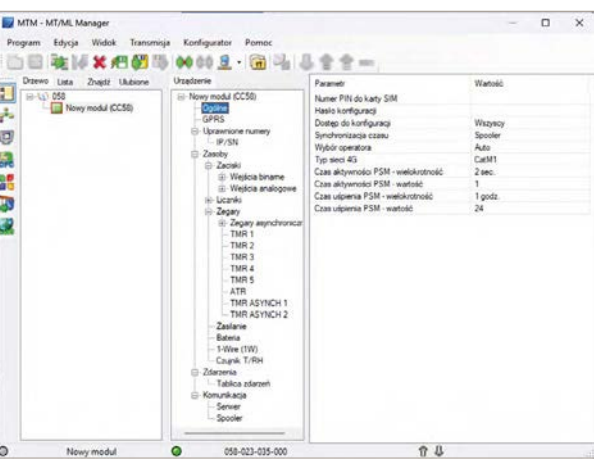
Czujnik temperatury i wilgotności (opcja)

Typowa dokładność temperatury	1 °C
Zakres pomiaru temperatury	-20 +60 °C
Typowa dokładność wilgotności względnej	3 %RH
Roboczy zakres wilgotności względnej	0–100 %RH

Opcje dodatkowe

Możliwość zamontowania karty MIM	
Uchwyt do wewnętrznej baterii litowej rozmiar D	

Oprogramowanie konfiguracyjne



Rysunki i wymiary (wszystkie wymiary w milimetrach)



MT-058

MT-221 – Brama komunikacyjna programowana w środowisku CODESYS®

WARRANTY
3
YEARS

CODESYS

PLC

SMS

4G

DIN RAIL

RS-232/485

4G

DO SPISU TREŚCI

- Programowalny sterownik PLC, bezpłatne środowisko programistyczne CODESYS®
- Wbudowany modem GSM 2G/4G Cat 1
- Technologia Dual-SIM (tryb pasywny) – dostęp do 2 niezależnych sieci GSM zapewnia redundancję infrastruktury transmisyjnej
- Port Ethernet 10Base-T/100Base-TX
- Port szeregowy RS-232/485 dla urządzeń zewnętrznych (izolacja galwaniczna)
- Diagnostyczne diody LED
- Redundantne wejścia zasilające
- Zegar czasu rzeczywistego (RTC)
- Rejestrator danych o rozdzielczości 0,1s
- Standardowe protokoły komunikacyjne (Modbus RTU, Modbus TCP, przezroczystość)
- Programowa obsługa portu szeregowego FlexSerial
- Zdalna konfiguracja, programowanie, diagnostyka i aktualizacja firmware (OTA)
- Konstrukcja przemysłowa, montaż na szynie DIN, zaciski śrubowe
- 3-letnia gwarancja

MT-221 umożliwia bezprzewodową integrację poprzez sieć 2G/4G urządzeń pomiarowych, sterowników PLC, układów wejść/wyjść, paneli operatorskich wyposażonych w port komunikacyjny RS-232/485 lub port Ethernet. Posiada środowisko wykonawcze CODESYS, dzięki czemu rozwiązanie łączy w sobie zaawansowane funkcje techniczne i łatwą obsługę. Może pełnić rolę lokalnego Mastera, który cyklicznie odczytuje urządzenia zewnętrzne o zdefiniowane przez użytkownika zasoby. W pamięci MT-221 tworzone jest zwierciadło zasobów urządzenia, pozwalające na wykrywanie alarmów, zmian wartości rejestrów odczytanych z zewnętrznych urządzeń. W oparciu o wewnętrzny program użytkownika wartości odczytane z urządzenia mogą być bezpośrednio poddane lokalnej analizie. Na podstawie wyników obliczeń moduł MT-221 może przekazać dane z obiektu wykorzystując pakietową transmisję danych lub krótkie wiadomości tekstowe SMS. Moduł może współpracować z systemem nadrzędnym kierującym pakietami danych z pytaniami, bądź rozkazami na jego zdefiniowany port szeregowy lub port Ethernet.

Oprócz funkcji komunikacyjnych i obliczeniowych jednostka MT-221 umożliwia rejestrowanie dużych ilości danych. Posiada również redundantne wejścia zasilające o szerokim zakresie napięć zasilania (11–30 V DC).

Przemysłowa konstrukcja urządzenia, integralny modem 2G/4G, możliwość programowania przez użytkownika, odpowiednio dobrane parametry techniczne oraz łatwe w użyciu narzędzia konfiguracyjne to atuty MT-221 w zastosowaniach bezprzewodowej telemetrii, nadzoru, diagnostyki, sterowania oraz zdalnego odczytu zużycia mediów.

Zasoby:

- CODESYS RUNTIME SYSTEM (RTS) z dostępnymi zasobami pamięci 256kB FLASH, 32kB RAM
- Integralny, wielozakresowy modem komunikacyjny 2G/4G



- Tworzenie programu użytkownika przy użyciu bezpłatnego CODESYS Development System zgodnie z IEC 61131-3, z możliwością debugowania
- Port Ethernet 10Base-T/100Base-TX
- 1 port RS-485/RS-232 do dołączania urządzeń zewnętrznych, izolowany galwanicznie (monitorowanie, diagnostyka)
- 2 redundantne wejścia zasilające
- Wewnętrzna pamięć nieulotna na dane konfiguracyjne z możliwością zdalnej aktualizacji
- Rejestrator pracy urządzenia w pamięci Flash (8 MB)
- Dual-SIM
- Zegar czasu rzeczywistego RTC
- Sygnalizacja pracy LED
- Port USB-C do konfiguracji

Funkcjonalność:

- Tryby komunikacji:
 - » 2G/4G Cat 1 – transmisja pakietowa
 - » SMS
 - » Ethernet
- Dostęp do zasobów wewnętrznych modułu standardowym protokołem MODBUS
- Możliwość transmisji danych do/z urządzeń podłączonych do portu komunikacyjnego
- Inteligentny routing pakietów i praca Multimaster w trybie MODBUS
- Rosyłanie pakietów w trybie przezroczystym
- Możliwość samodzielnego zgłaszania zdarzeń alarmowych (unsolicited messages) w wyniku zmiany wewnętrznej flagi lub też spełnienia funkcji logicznej
- Zabezpieczenie przed nieuprawnionym dostępem w postaci listy uprawnionych numerów telefonów i IP, opcjonalnie hasło do konfiguracji
- Rejestrator z rozdzielczością 0,1 sek.

- Możliwość wysyłania SMS w wyniku zaistnienia sytuacji alarmowej, od flagi lub według harmonogramu
- Dynamiczne wstawianie wartości zmiennych w tekst wiadomości SMS
- Możliwość zdalnej zmiany parametrów konfiguracyjnych i programu wewnętrznego modułu
- Przyjazne narzędzia konfiguracyjne
- Łatwa integracja z oprogramowaniem centrum serwisowego
- Diody LED (status modułu, aktywność komunikacji GSM, poziom sygnału GSM, aktywność DATA, aktywność komunikacji szeregowej, aktywność portu USB, aktywność portu Ethernet, aktywność wejścia zasilania)
- Rozłączalne listwy zaciskowe
- Zasilanie 12 V DC/24 V DC
- Montaż na szynie DIN

Ogólne

Wymiary (dł. x szer. x wys.)	105 x 86 x 59 mm
Waga	268 g
Sposób mocowania	Szyna DIN 35mm
Temperatura pracy	-20°C do +55°C
Klasa ochrony	IP 20

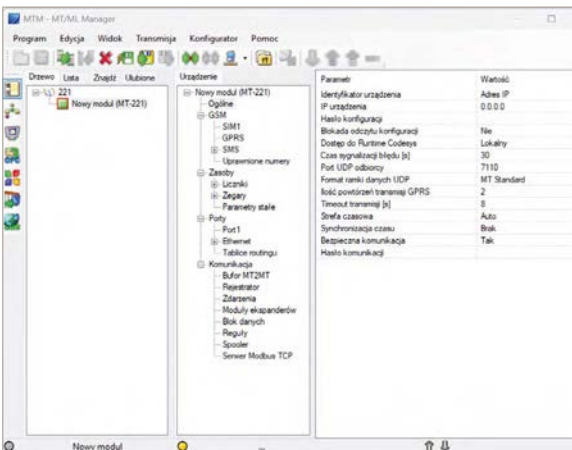
Modem radiowy

Producent i typ	SIMCom A7672G
Region	globalny
Pasma 2G	850/900/1800/1900 MHz
Pasma 4G	Band: 1, 2, 3, 4, 5, 7, 8, B12, 13, 17, 18, 19, 20, 25, 26, 28, 38, 39, 40, 41, 66
Złącze anteny zewnętrznej	50 Ω, SMA-F

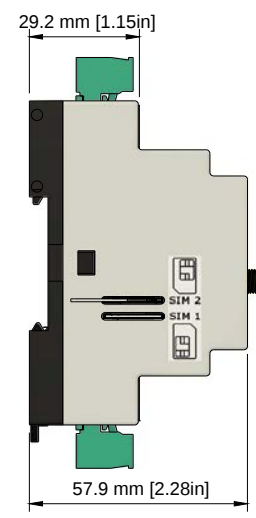
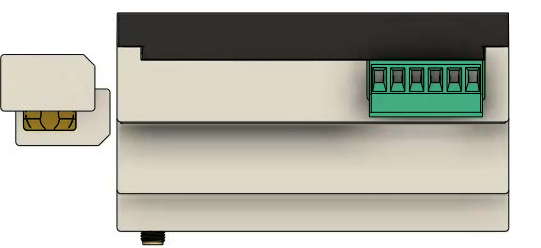
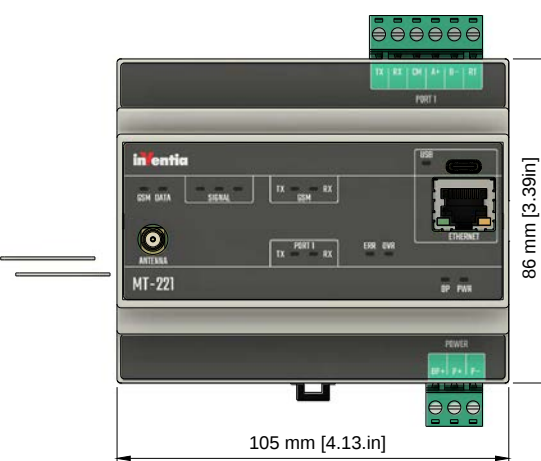
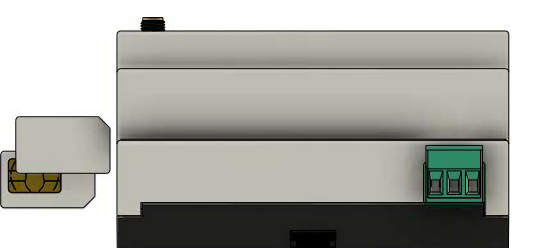
Zasilanie

Napięcie stałe DC (nom. 12/24 V)	11 – 30 V DC		
Prąd zasilania (typ.) @ 25°C	Spoczynkowy	Aktywny (Praca)	Maksymalny
12 V DC	0,04 A	0,1 A	1,0 A
24 V DC	0,02 A	0,05 A	0,5 A

Oprogramowanie konfiguracyjne



Rysunki i wymiary (wszystkie wymiary w milimetrach)



MT-221

MTX-2050 v4 – 2G/LTE brama komunikacyjna z portem Ethernet



- Wewnętrzny modem 4G LTE Cat. 1 z obsługą 2G
- Port Ethernet: 100Base-TX/10Base-T z auto MDI/MDI-X
- Technologia Dual-SIM (tryb pasywny) – dostęp do 2 niezależnych sieci GSM zapewnia redundancję infrastruktury transmisyjnej
- Konfiguracja za pomocą dedykowanego interfejsu WebGUI i SSH
- Wbudowany interfejs WebGUI z funkcją wizualizacji danych
- 2 porty szeregowo do komunikacji z urządzeniami zewnętrznymi:
 - izolowany RS-232/485
 - izolowany RS-485
- 4 wejścia binarne/2 konfigurowalne jako wyjścia binarne
- Rejestrator danych (obsługa kart microSD)
- Konwerter protokołów (obsługuje Modbus RTU, Modbus TCP, UDP, MQTT)
- Wbudowana funkcjonalność Modbus Master i Slave
- Opcjonalny wbudowany port wM-Bus, obsługa do 20 urządzeń wM-Bus
- Routing pakietów Modbus
- Obsługa protokołów SNMP v2c/v3 i SNMP Trap
- Diagnostyczne diody LED
- Zaawansowana autodiagnostyka z mechanizmem Watchdog
- Bramka SMS

MTX-2050 v4 to nowoczesna przemysłowa brama telemetryczna przeznaczona do realizacji zdalnego monitoringu, akwizycji danych oraz integracji urządzeń automatyki w sieciach LTE. Łączy funkcje bramy komunikacyjnej, konwertera protokołów oraz koncentratora danych, umożliwiając budowę niezawodnych systemów komunikacyjnych dla infrastruktury krytycznej: energetyki, ciepłownictwa, gospodarki wodno-ściekowej, przemysłu i infrastruktury komunalnej. Dzięki obsłudze interfejsów Ethernet, RS-232, RS-485, M-Bus oraz wM-Bus urządzenie może współpracować zarówno z nowoczesnymi systemami automatyki, jak i istniejącą infrastrukturą pomiarową.

MTX-2050 v4 umożliwia lokalne gromadzenie, przetwarzanie i udostępnianie danych pochodzących z urządzeń polowych. Wbudowane funkcje Modbus Master i Slave, konwersja protokołów, routing danych oraz mechanizmy lustrzanego odwzorowania zasobów pozwalają na integrację wielu urządzeń w ramach jednej platformy komunikacyjnej. Urządzenie może cyklicznie odczytywać dane, wykrywać zmiany stanów i alarmy, realizować logikę zdarzeniową oraz rejestrować informacje wraz ze znacznikiem czasu. Dzięki temu możliwe jest skrócenie czasu reakcji systemu oraz zwiększenie niezawodności procesów monitoringu i sterowania.

Wbudowany modem LTE Cat.1 z obsługą sieci 2G oraz technologia Dual-SIM zapewniają stabilną komunikację nawet w lokalizacjach o zmiennych warunkach transmisyjnych. Rozbudowane funkcje bezpieczeństwa, obejmujące obsługę VPN, SNMPv3, mechanizmy uwierzytelniania oraz zaawansowaną kontrolę dostępu, umożliwiają bezpieczną integrację z systemami nadrzędnymi. Dodatkowo funkcje zdalnej konfiguracji, diagnostyki i aktualizacji oprogramowania pozwalają ograniczyć koszty utrzymania rozproszonych instalacji.



- Wbudowany procesor zdarzeń do reguł transmisji danych
- Zdalna konfiguracja, programowanie, diagnostyka i aktualizacja oprogramowania przez sieć 2G/LTE
- Redundantne wejścia zasilające
- Opcjonalna karta MIM
- Zasilanie 12-48 V DC
- Zegar czasu rzeczywistego (RTC)
- Konstrukcja przemysłowa, montaż na szynie DIN, złącza śrubowe

Wersja v4 została rozszerzona o obsługę urządzeń M-Bus oraz opcjonalny interfejs wM-Bus, umożliwiając integrację liczników energii elektrycznej, ciepła, wody i gazu. Urządzenie obsługuje automatyczne wykrywanie urządzeń M-Bus, konfigurację adresów komunikacyjnych oraz selektywne udostępnianie danych do systemów nadrzędnych. Dzięki połączeniu zaawansowanych funkcji komunikacyjnych, obsługi Smart Meteringu i lokalnego przetwarzania danych MTX-2050 v4 stanowi uniwersalną platformę dla nowoczesnych systemów telemetrycznych, IoT i przemysłowych.

Zasoby:

- Port Ethernet 100Base-TX/10Base-T z funkcją auto MDI/MDI-X
- Izolowany port szeregowy RS-232 lub RS-485
- Izolowany port szeregowy RS-485
- 4 wejścia binarne/2 konfigurowalne wyjścia binarne
- Port USB-C do lokalnej konfiguracji i programowania
- Flagi wewnętrzne i rejestry
- Zdalna aktualizacja oprogramowania wewnętrznego (FOTA)
- Rejestrator danych obsługujący kartę microSD
- Możliwość wlutowania karty MIM
- Gniazda dla 2 kart SIM (redundancja sieci 2G/4G)
- Zegar RTC z zewnętrznymi funkcjami synchronizacji
- Zintegrowany interfejs dla kart microSD/SDHC/SDXC do 256 GB

Funkcjonalność:

- Standard transmisji: transmisja pakietowa 2G/LTE, SMS, Ethernet, MQTT (Publisher)
- Funkcjonalność sieciowa: IPv4, przekierowanie portów, NAT, DHCP klient/serwer/relay
- Zarządzanie i wizualizacja danych przez WebGUI
- Dostęp do Secure Shell (SSH)

- Bezpieczna zdalna aktualizacja oprogramowania
- Redundantne partycje rootfs
- Konwerter protokołów (obsługuje Modbus RTU, Modbus TCP, UDP, MQTT)
- Dostęp do zdalnych zasobów za pomocą standardowych protokołów Modbus RTU i Modbus TCP
- Routing pakietów i obsługa Multimaster w trybie Modbus
- Transmisja danych z urządzeń zewnętrznych podłączonych do portu szeregowego i portu Ethernet, portu M-Bus, wM-Bus
- Mapowanie zasobów zewnętrznych (lustrzane odbicie) dla wykrywania i wyzwalania zdarzeń
- Bufor MT2MT do bezpośredniego udostępniania danych między innymi modułami telemetrycznymi MT
- Multitransmisja w trybie przezroczystym
- Wysyłka danych na broker MQTT
- Obsługa protokołu SNMP v2c/v3 (w tym SNMP Trap i funkcja odpytywania). Moduł działa jako agent SNMP – urządzenie, które może być odpytywane przez serwer i może wysyłać zdarzenia spontanicznie
- Zdalna konfiguracja i programowanie przez sieć 2G/LTE
- Wsparcie Zabbix
- Transmisja oparta na zdarzeniach wyzwalana zmianą stanu wejścia/wyjścia binarnego, stanem wew. flagi

Ogólne

Wymiary (L x W x H)	105 x 86 x 59 mm
Waga	200 g
Sposób mocowania	DIN Rail 35 mm
Temperatura pracy	-20° do +55 °C
Stopień ochrony	IP20
Wilgotność	do 95 %, bez kondensacji
Wskaźniki stanu	15 zielonych, 1 czerwony

System

Procesor	Cortex A5 500 MHz
System operacyjny	Linux
Pamięć operacyjna (RAM)	256 MB
Pamięć wewnętrzna (FLASH)	512 MB

Modem

Typ	SIMCOM A7672G
Region	Globalny
Pasmo 2G	850/900/1800/1900 MHz
Pasmo LTE	Band: 1, 2, 3, 4, 5, 7, 8, 12, 13, 18, 19, 20, 25, 26, 28, 38, 39, 40, 41, 66
Złącze do anteny zewnętrznej	SMA-F 50 Ω

Interfejs wM-Bus

Typ	EFR32ZG23
Region	Europa
Typ komunikacji	S,T lub C
Bezpieczeństwo	Profile A i B (szyfrowanie mod 5 i 7)
Standard	OM5v4.5.1, EN 13757-3/-4/-7
Częstotliwość	868,95 MHz
Czułość odbiornika	> -108dBm
Złącze do anteny wM-Bus	SMA-F 50 Ω
Ilość obsługiwanych urządzeń	do 20

- Rejestrator danych z zapisem na karcie microSD
- Konfigurowalne wiadomości SMS wyzwalane przez alarmy i dynamiczne wartości wstawiane w tekście SMS, obsługa nazw symbolicznych i makr
- Konfigurowalne zabezpieczenia dostępu – lista autoryzowanych adresów IP i numerów telefonów
- Obsługa firewall (iptables)
- Obsługa wielopoziomowych uprawnień użytkownika w celu zapewnienia bezpieczeństwa transmitowanych danych
- Montaż na szynie DIN
- Wbudowana zaawansowana autodiagnostyka
- Złączki śrubowe
- Przyjazne dla użytkownika narzędzia konfiguracyjne i driver komunikacyjny (obsługa OPC i RDB) – MTDataProvider
- Wsparcie Simple Network Time Protocol (SNTP)

Bezpieczeństwo:

- Dostępne mechanizmy bezpieczeństwa sieci VPN: OpenVPN, STRONGSWAN (IPsec)
- RADIUS (Remote Authentication Dial-In User Service)
- Uwierzytnienie na portach oparte na 802.1X
- Klucze prywatne przechowywane w TPM2
- Wykrywanie i zapobieganie włamaniom SNORT

Port M-Bus

Typ portu	M-Bus
Maksymalna ilość urządzeń	4
Prędkość transmisji	300 do 9600 Bodów
Standardowe obciążenie urządzenia peryferyjnego	do 1,5 mA

Wejścia binarne IQ1, IQ2, I3, I4

Zakres napięcia wejściowego	0–58 V
Stan ON (1)	>8 V @ 2 m
Stan OFF (0)	<5 V @ 1,5 mA
Maksymalna częstotliwość impulsów	2 kHz
Minimalna długość wykrywanego impulsu	0,25 ms

Wyjścia binarne IQ1, IQ2

Zakres napięcia zasilania VQ+	7–53 V
Zalecany prąd obciążenia	0,2 A
Maksymalny prąd obciążenia	0,5 A
Ograniczenie prądowe (max.)	1,5 A
Spadek napięcia (VQ+ - IQx)	@0,2 A <1,9 V 1,25 V (typ.) @0,5 A <3,4 V 1,9 V (typ.)

Interfejsy

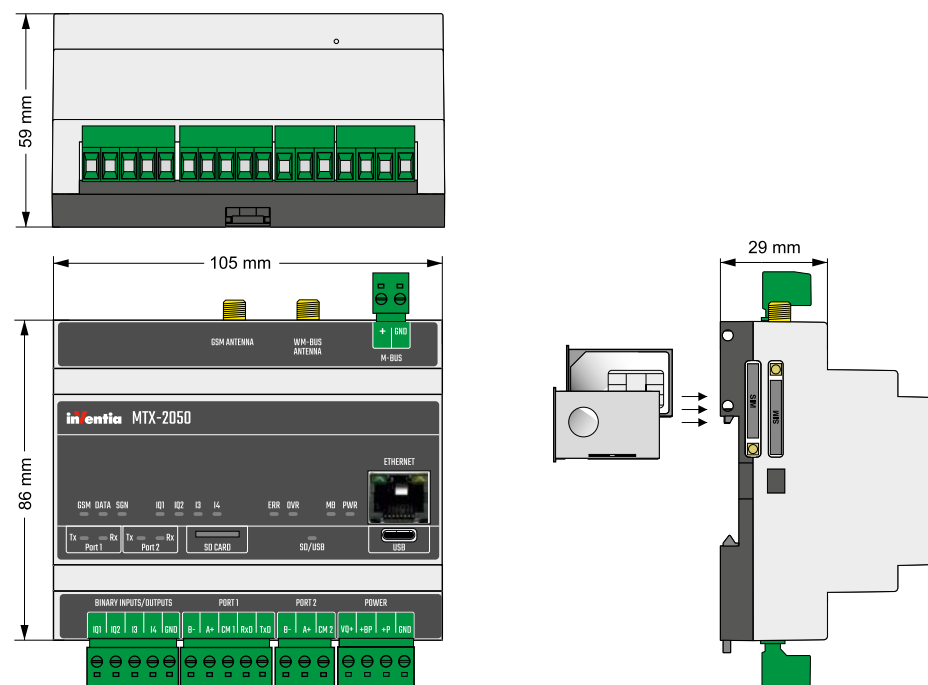
Ethernet	1 x RJ45
Porty szeregowo	1 x RS-232/RS-485 izolowany combo 1 x RS-485 izolowany
Interfejs USB	USB 2.0, USB-C
Port karty SD	micro-SD/SDHC/SDXC do 256 GB

Zasilanie

Napięcie stałe DC 12V/24V/48V	10,8–53 V
Prąd wejściowy (@ 25°C)	Idle Active Max. 12 V DC 0,15 A 0,33 A 2,00 A 24 V DC 0,07 A 0,16 A 1,00 A 48 V DC 0,04 A 0,09 A 0,50 A

MTX-2050 v4

Rysunki i wymiary (wszystkie wymiary w milimetrach)



Przetworniki ciśnienia A-10/S-20

Przetwornik ciśnienia przeznaczony do zastosowań w branży wodno-kanalizacyjnej umożliwia niezawodny monitoring ciśnienia w sieciach wodociągowych, przepompowniach ścieków, hydroforniach, stacjach uzdatniania wody oraz układach pompowych. Zapewnia bieżącą kontrolę parametrów pracy instalacji i wspiera szybkie wykrywanie nieprawidłowości.

Szeroki zakres pomiarowy oraz standardowe sygnały wyjściowe pozwalają na łatwą integrację z systemami automatyki, telemetry i zdalnego monitoringu obiektów wod-kan. Dokładny pomiar umożliwia wykrywanie spadków ciśnienia, przeciążeń oraz awarii pomp i rurociągów. Wykonanie ze stali nierdzewnej gwarantuje odporność na trudne warunki eksploatacyjne i długotrwałą, bezawaryjną pracę. Różnorodność przyłączy ułatwia montaż zarówno w nowych, jak i modernizowanych instalacjach wodociągowych i kanalizacyjnych.



Antena LTE Heavy-duty

Wytrzymała antena LTE typu heavy-duty przeznaczona do pracy w systemach monitoringu i telemetry obiektów wodno-kanalizacyjnych, takich jak przepompownie, studnie pomiarowe, zbiorniki, hydrofornie czy stacje uzdatniania wody. Umożliwia stabilną transmisję danych z urządzeń pracujących w terenie, wspierając zdalny nadzór nad pracą instalacji. Solidna konstrukcja z żywicy poliuretanowej i stali nierdzewnej oraz szeroki zakres temperatur pracy od -45°C do +85°C sprawiają, że antena dobrze sprawdza się w wymagających warunkach zewnętrznych.



Czujnik krańcowy otwarcia włazu

Czujnik krańcowy przeznaczony do sygnalizacji otwarcia włazu w obiektach wodno-kanalizacyjnych, takich jak przepompownie, studnie, komory technologiczne czy zbiorniki. Dzięki elastycznemu trzpieniowi typu Wobble Stick umożliwia wykrywanie zmiany położenia pokrywy lub elementu ruchomego, a konfiguracja styków 1NC/1NO pozwala na łatwą integrację z systemem monitoringu lub alarmowania. Stopień ochrony IP67 oraz szeroki zakres temperatur pracy sprawiają, że czujnik dobrze sprawdza się w wymagających warunkach terenowych i przemysłowych.



MT-UPS-1 - mikroprocesorowy moduł podtrzymania zasilania

MT-UPS-1 jest nowoczesnym, sterowanym cyfrowo zasilaczem buforowym, zapewniającym bezprzerwowe podtrzymanie zasilania modułu telemetrycznego i zewnętrznych odbiorników energii w przypadku zaniku napięcia z podstawowego źródła zasilania. Konstrukcja urządzenia przewiduje współpracę z dowolnym zasilaczem sieciowym 24 V DC (podstawowe źródło zasilania) oraz zewnętrznym akumulatorem SLA (awaryjne źródło zasilania) o napięciu nominalnym 12 V.



Inteligentny moduł zasilania zewnętrznego MT-CPV

MT-CPV to inteligentny moduł zasilania stworzony z myślą o niezawodnej pracy bateryjnych systemów telemetrycznych w terenie. Wykorzystuje zaawansowany algorytm MPPT, który maksymalizuje efektywność pozyskiwania energii z paneli fotowoltaicznych, wydłużając czas autonomicznej pracy urządzeń. Wbudowane podtrzymanie akumulatorowe oraz możliwość współpracy z różnymi źródłami zasilania zapewniają ciągłość działania nawet w wymagających warunkach eksploatacyjnych.



Kompaktowy zasilacz impulsowy

Kompaktowy zasilacz impulsowy do montażu na szynie DIN przeznaczony jest do zastosowań w: automatyce budynkowej, przemysłowej i systemach sterowania. Ma wąską obudowę 52,5 mm, wejście 85–264 V AC. Zapewnia moc do 60 W, wysoką sprawność do 91%, pracę w zakresie od -30°C do +70°C oraz zabezpieczenia przed zwarcieniem, przeciążeniem i przepięciem. To praktyczne rozwiązanie do rozdzielnic i szaf sterowniczych.



Zastosowania telemetrii w branży wod-kan

Nowoczesne przedsiębiorstwa wodociągowo-kanalizacyjne wymagają stałej kontroli nad rozproszoną infrastrukturą. Systemy telemetryczne Inventii integrują przepompownie, ujęcia wody, studnie głębinowe, zbiorniki, stacje uzdatniania oraz obiekty pomiarowe w jeden ekosystem zdalnego nadzoru.

Monitoring zestawów hydroforowych



Nadzór nad pracą zestawów hydroforowych oraz kontrola parametrów hydraulicznych sieci:

- pomiar ciśnienia w sieci oraz bieżąca kontrola stabilności parametrów hydraulicznych,
- nadzór nad falownikami pomp, ich stanami pracy, sygnałami awaryjnymi i parametrami regulacji,
- kontrola regulatorów PID odpowiedzialnych za utrzymanie zadanego ciśnienia w instalacji,
- odczyt danych ze sterownika zestawu hydroforowego i monitorowanie pracy układu pompowego,
- kontrola położenia przełączników do lokalnego sterowania oraz trybów pracy urządzeń,
- nadzór nad zabezpieczeniami nadprądowymi, przeciążeniowymi i technologicznymi,
- sygnalizacja alarmów, awarii oraz stanów wymagających interwencji obsługi,
- rejestracja zdarzeń i analiza trendów parametrów, w tym zmian ciśnienia, pracy pomp oraz stanów układu regulacji.

Dane z zestawu hydroforowego mogą być przesyłane do systemu SCADA lub platformy zdalnego nadzoru z wykorzystaniem bezpiecznych mechanizmów transmisji. Umożliwia to bieżącą kontrolę pracy obiektu, szybką diagnostykę nieprawidłowości oraz nadzór nad rozproszonymi instalacjami podnoszenia ciśnienia.

Monitoring sieci wodociągowej i komór pomiarowych



Zdalny odczyt parametrów pracy sieci wodociągowej oraz wybranych parametrów jakości wody:

- pomiar przepływu i ciśnienia w sieci oraz bieżąca kontrola parametrów hydraulicznych,
- pomiar poziomu medium w zbiornikach, komorach lub wybranych punktach pomiarowych,
- analiza pH, temperatury i przewodności wody lub ścieków, zależnie od charakteru obiektu,
- detekcja otwarcia wjazdu/wejścia na obiekt,
- współpraca z przepływomierzami i przetwornikami pomiarowymi,
- odczyt danych z urządzeń pomiarowych z wykorzystaniem protokołu Modbus RTU,
- rejestracja wartości bieżących, stanów granicznych oraz zdarzeń wymagających reakcji obsługi,
- sterowanie pompami i zasuwami według zaprogramowanego algorytmu pracy,
- przesyłanie danych do systemu SCADA lub platformy zdalnego nadzoru w celu analizy pracy sieci i szybkiego wykrywania nieprawidłowości.

Protokół Modbus RTU umożliwia cyfrową komunikację z urządzeniami pomiarowymi, w tym z przepływomierzami i przetwornikami parametrów jakościowych. W przypadku obiektów bez dostępu do zasilania stacjonarnego możliwe jest zastosowanie przepływomierzy bateryjnych oraz modułów telemetrycznych przystosowanych do pracy z zewnętrznym pakietem baterii.

Monitoring studni głębinowych i ujęć



Zdalny nadzór nad pracą pomp oraz monitoring parametrów eksploatacyjnych ujęć:

- sterowanie pracą pomp głębinowych na podstawie poziomu wody, ciśnienia lub innych parametrów technologicznych,
- monitoring poziomu wody w studni, zbiorniku lub układzie współpracującym z ujęciem,
- pomiar ciśnienia w instalacji, w tym kontrola ciśnienia przed i za filtrami lub w rurociągu tłocznym,
- analiza parametrów pracy pomp, stanów urządzeń oraz sygnałów eksploatacyjnych,
- kontrola trybów pracy, gotowości urządzeń oraz sygnałów awaryjnych,
- nadzór nad zabezpieczeniami elektrycznymi, przeciążeniowymi i technologicznymi,
- rejestracja alarmów, zdarzeń oraz stanów wymagających interwencji obsługi,
- przesyłanie danych z ujęcia do systemu SCADA lub platformy zdalnego nadzoru, w celu bieżącej kontroli pracy obiektu.

Moduł telemetryczny zabudowany w szafie sterowniczej przy studni umożliwia lokalny i zdalny podgląd parametrów pracy ujęcia, diagnostykę stanów awaryjnych oraz sterowanie pompą głębinową zgodnie z zaprogramowanym algorytmem. Dzięki temu możliwy jest skuteczny nadzór nad rozproszonymi ujęciami wody bez konieczności stałej obecności obsługi na obiekcie.

Monitoring poziomu wody w zbiornikach



Zdalny pomiar poziomu oraz automatyczne sterowanie napełnianiem:

- pomiar poziomu w retencji, zbiornikach wody czystej lub innych obiektach magazynowania medium,
- bieżące monitorowanie stanów minimalnych, maksymalnych oraz alarmowych,
- sterowanie pompami i zasuwami odpowiedzialnymi za napełnianie lub opróżnianie zbiorników,
- automatyczne zarządzanie procesem napełniania według zaprogramowanego algorytmu pracy,
- kontrola stanów urządzeń wykonawczych, przełączników oraz sygnałów awaryjnych,
- sygnalizacja przekroczeń poziomu, awarii urządzeń oraz stanów wymagających interwencji obsługi,
- archiwizacja i analiza trendów poziomu wody, pracy pomp oraz cykli napełniania,
- przesyłanie danych do systemu SCADA lub platformy zdalnego nadzoru w celu bieżącej kontroli pracy obiektu.

Autonomiczna praca obiektu nawet w przypadku przerwy w komunikacji pozwala na utrzymanie procesu napełniania lub opróżniania zbiornika zgodnie z lokalnym algorytmem sterowania. Dzięki temu obiekt może bezpiecznie kontynuować pracę, a dane i alarmy mogą zostać przekazane do systemu nadrzędnego po przywróceniu łączności.

Monitoring przepompowni ścieków



Zdalny nadzór i sterowanie pracą przepompowni oraz tłoczni ścieków:

- sterowanie pracą pomp, realizowane przez moduł telemetryczny zabudowany w szafie sterowniczej,
- automatyczna kontrola pracy pomp zgodnie z zaprogramowanym algorytmem,
- pomiar poziomu ścieków i wykorzystanie tej informacji do sterowania oraz alarmowania,
- kontrola falowników i soft-startów stosowanych przy pompach o większej mocy, odczyt parametrów pracy układów napędowych oraz diagnostyka ich stanów,
- nadzór nad zabezpieczeniami elektrycznymi, przeciążeniowymi i technologicznymi,
- kontrola stanów przełączników, sygnałów awaryjnych i gotowości urządzeń do pracy,
- sygnalizacja alarmów, awarii oraz stanów wymagających interwencji obsługi,
- możliwość współpracy z panelem graficznym HMI wyposażonym w ekran dotykowy,
- przesyłanie danych z obiektu do systemu zdalnego nadzoru w celu bieżącej kontroli pracy przepompowni.

Komunikacja z urządzeniami obiektowymi przez RS-232/RS-485 lub Ethernet umożliwia integrację z automatyką przepompowni, falownikami, soft-startami, panelem operatorskim oraz urządzeniami pomiarowymi. Dzięki temu możliwy jest zarówno lokalny podgląd parametrów pracy obiektu, jak i zdalny nadzór nad rozproszonymi przepompowniami oraz tłoczniami ścieków.

Telemetria dla stacji uzdatniania wody



Praca w charakterze koncentratora danych i/lub bramy komunikacyjnej pomiędzy sterownikami PLC a systemem SCADA:

- odczyt danych technologicznych ze sterownika PLC, realizującego proces sterowania stacją,
- bieżące monitorowanie pracy urządzeń technologicznych zabudowanych na obiekcie,
- kontrola pracy pomp, układów dozowania, filtracji oraz innych elementów procesu uzdatniania,
- pomiar i rejestracja podstawowych parametrów pracy stacji, takich jak ciśnienie, przepływ, poziom wody oraz stany urządzeń,
- nadzór nad zabezpieczeniami elektrycznymi, przeciążeniowymi i technologicznymi,
- kontrola stanów przełączników, sygnałów awaryjnych i gotowości urządzeń do pracy,
- sygnalizacja alarmów, awarii oraz stanów wymagających interwencji obsługi,
- możliwość współpracy z panelem graficznym HMI wyposażonym w ekran dotykowy,
- przesyłanie danych z obiektu do systemu SCADA do bieżącej kontroli pracy stacji uzdatniania wody,
- transmisja danych w trybie zdarzeniowym według zdefiniowanych reguł.

Komunikacja z urządzeniami obiektowymi przez RS-232/RS-485 lub Ethernet umożliwia integrację z automatyką stacji uzdatniania wody, sterownikiem PLC, panelem operatorskim HMI, urządzeniami pomiarowymi oraz elementami wykonawczymi procesu technologicznego. Dzięki temu możliwy jest zarówno lokalny podgląd parametrów pracy obiektu, jak i zdalny nadzór nad pracą rozproszonych stacji uzdatniania wody.

Regulacje i standardy istotne dla cyberodpornej telemetrii wod-kan

Przybornik dla przedsiębiorstw wodociągowo-kanalizacyjnych, projektantów i integratorów

1. Cel dokumentu

Celem dokumentu jest krótkie uporządkowanie najważniejszych regulacji i standardów, które mogą wpływać na cyberodporność telemetrii, SCADA, usług chmurowych, transmisji danych, urządzeń telemetrycznych oraz współpracy z dostawcami technologii.

Dokument nie przesądza, które obowiązki mają zastosowanie do konkretnego przedsiębiorstwa, produktu, usługi lub projektu. Nie zastępuje analizy prawnej, audytu bezpieczeństwa ani oceny zgodności produktu, ani nie stanowi zamkniętego katalogu regulacji i norm, którym podlegają przedsiębiorstwa wod-kan.

Ma pomóc w szybkim zorientowaniu się:

- jakie regulacje i standardy warto znać,
- czego zasadniczo dotyczą,
- dlaczego mogą być istotne dla wod-kan,
- gdzie szukać źródeł wymagań,
- jakich obszarów organizacji mogą dotyczyć.

2. Mapa wpływu regulacji i standardów

Kluczowe jest zrozumienie, że regulacje i standardy nie działają w izolacji. W praktyce wzajemnie się uzupełniają i wpływają jednocześnie na kilka obszarów organizacji:

- zarządzanie ryzykiem,
- ciągłość działania,
- obsługę incydentów,
- zakupy i łańcuch dostaw,
- telemetrię, OT i SCADA,
- usługi chmurowe i dane,
- bezpieczeństwo produktów cyfrowych,
- jakość i dostępność usług świadczonych odbiorcom.

3. Przybornik regulacyjno-normatywny

Status prawny ma charakter orientacyjny. Ostateczny zakres obowiązków zależy od roli podmiotu, wielkości przedsiębiorstwa, rodzaju świadczonej usługi, modelu wdrożenia, wykorzystanych technologii oraz właściwych przepisów krajowych.

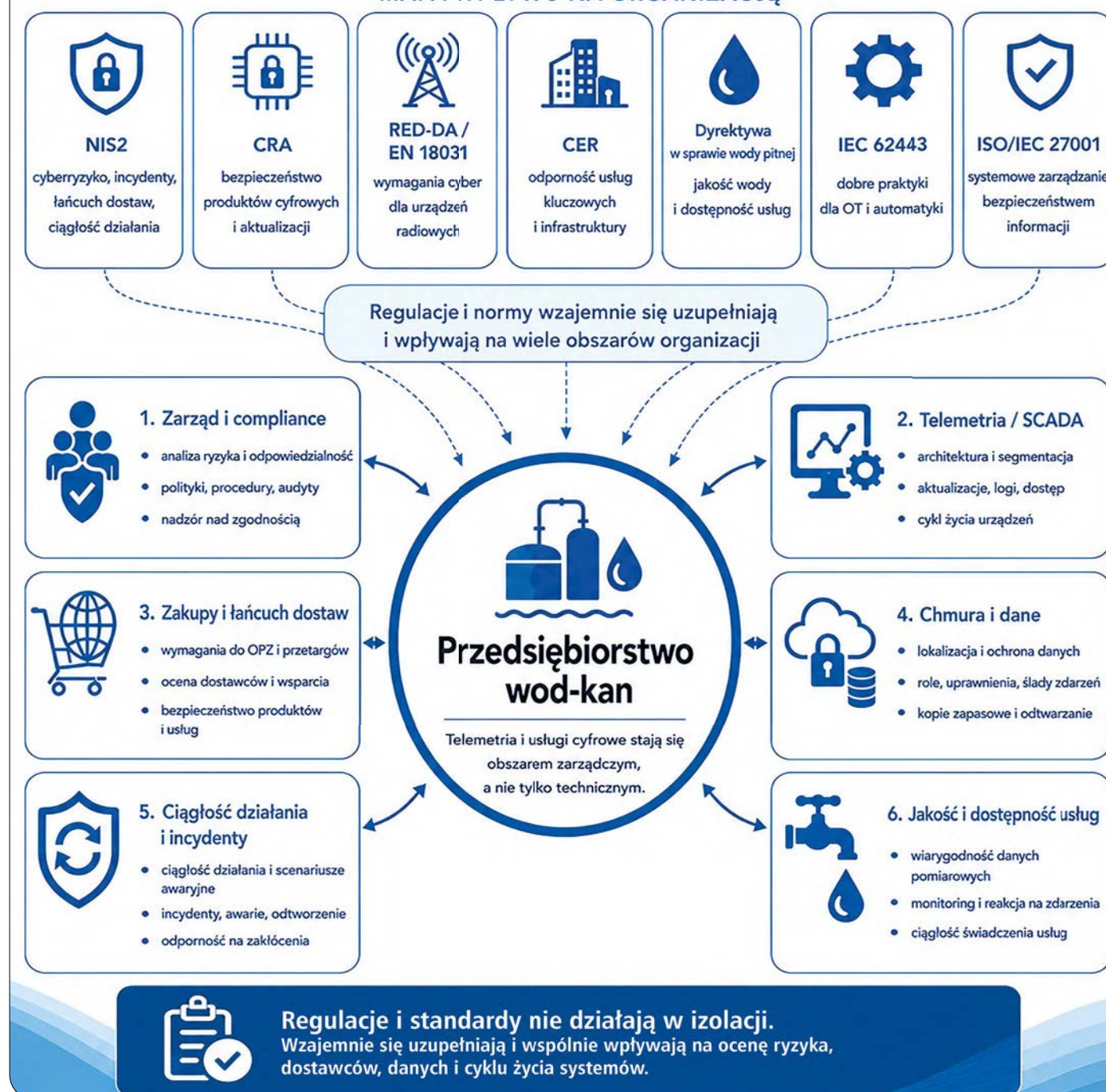
Prawnie obligatoryjne oznacza, że dana regulacja może nakładać obowiązki bezpośrednio na określone podmioty, produkty, usługi lub rodzaje działalności.

Prawnie obligatoryjne warunkowo oznacza, że obowiązek zależy od spełnienia określonych przesłanek, na przykład rodzaju produktu, wykorzystania usługi chmurowej, przetwarzania danych, użycia systemu AI albo roli danego podmiotu.

Fakultatywne / dobra praktyka oznacza, że standard sam w sobie zwykle nie jest powszechnie obowiązującym prawem, ale może stać się wymaganiem umownym, przetargowym, projektowym lub audytowym.

Jak regulacje i standardy wpływają na przedsiębiorstwo wod-kan

— MAPA WPŁYWU NA ORGANIZACJĘ —



Regulacja / standard	Znaczenie dla wod-kan i co konkretnie sprawdzić
NIS2 – Dyrektywa (UE) 2022/2555 oraz KSC	Status: prawnie obligatoryjne dla podmiotów objętych przepisami. O co chodzi: zarządzanie ryzykiem cyberbezpieczeństwa, incydenty, ciągłość działania, bezpieczeństwo łańcucha dostaw i odpowiedzialność kierownictwa. Znaczenie dla wod-kan: w podmiotach objętych przepisami, telemetria, SCADA, dostęp zdalny, transmisja danych, usługi chmurowe i dostawcy technologii powinny być uwzględniane w analizie ryzyka oraz zarządzaniu ciągłością działania, jeżeli mają wpływ na bezpieczeństwo, dostępność lub ciągłość świadczenia usług wod-kan. Sprawdź: czy przedsiębiorstwo jest albo może być objęte obowiązkami KSC/NIS2 jako podmiot z sektora zaopatrzenia w wodę pitną, dystrybucji wody albo odprowadzania, usuwania i oczyszczania ścieków. Sprawdź wpis albo obowiązek wpisu do Wykazu KSC/S46, przypisanie osób kontaktowych, sposób zgłaszania incydentów do CSIRT NASK/CERT Polska oraz to, czy telemetria, SCADA, dostęp zdalny, transmisja danych, usługi chmurowe i integratorzy są ujęci w analizie ryzyka, procedurach ciągłości działania i obsłudze incydentów. Źródła: Dyrektywa (UE) 2022/2555, ustawa o krajowym systemie cyberbezpieczeństwa, Wykaz KSC/S46, cyber.gov.pl, CERT Polska / CSIRT NASK, formularz incydent.cert.pl.
CRA – Cyber Resilience Act – Rozporządzenie (UE) 2024/2847	Status: prawnie obligatoryjne dla producentów oraz - w określonym zakresie - importerów i dystrybutorów produktów z elementami cyfrowymi (urządzenia i oprogramowanie). O co chodzi: bezpieczeństwo produktów z elementami cyfrowymi, aktualizacje, obsługa podatności, dokumentacja, okres wsparcia i odpowiedzialność producenta. Znaczenie dla wod-kan: CRA nie nakłada obowiązków bezpośrednio na każde przedsiębiorstwo wod-kan jako użytkownika produktu, ale wpływa na sposób oceny urządzeń telemetrycznych, oprogramowania, firmware i narzędzi konfiguracyjnych. Przy zakupie lub modernizacji systemu warto zwracać uwagę na producenta, cykl życia produktu, deklarowany okres wsparcia, aktualizacje, obsługę podatności, dokumentację bezpieczeństwa i możliwość bezpiecznej konfiguracji. Rozporządzenie obowiązuje i jest wdrażane etapami. Obowiązki dotyczące zgłaszania istotnych incydentów i aktywnie wykorzystywanych podatności zaczną mieć znaczenie od września 2026 roku, a pełne wymagania produktowe od grudnia 2027 roku. Sprawdź: czy oferowane urządzenie, oprogramowanie SCADA, narzędziowe lub usługa powiązana mają wskazanego producenta i podmiot odpowiedzialny za aktualizacje, obsługę podatności, dokumentację oraz okres wsparcia. Sprawdź, czy producent deklaruje cykl życia produktu, sposób informowania o aktualizacjach bezpieczeństwa, sposób zgłaszania podatności, dokumentację bezpiecznej konfiguracji oraz zasady zakończenia wsparcia produktu. Źródła: Rozporządzenie (UE) 2024/2847, dokumentacja producenta, deklarowany okres wsparcia, możliwość uzyskiwania informacji o aktualizacjach, polityka obsługi podatności, dokumentacja bezpiecznej konfiguracji, przyszłe normy zharmonizowane.
CER – Dyrektywa (UE) 2022/2557 o odporności podmiotów krytycznych	Status: prawnie obligatoryjne dla podmiotów uznanych za krytyczne. O co chodzi: odporność podmiotów krytycznych i usług kluczowych na zakłócenia, awarie, zagrożenia fizyczne, organizacyjne i operacyjne. Znaczenie dla wod-kan: CER nie reguluje telemetrii bezpośrednio, ale wzmacnia znaczenie odporności, ciągłości działania, monitoringu, alarmowania i reagowania na zakłócenia. Telemetria może wspierać odporność przedsiębiorstwa wod-kan przez szybsze wykrywanie awarii, utraty łączności, zaniku zasilania, nietypowych stanów pracy obiektów oraz dokumentowanie przebiegu zdarzeń i reakcji służb. Sprawdź: które obiekty, procesy i usługi są najważniejsze dla ciągłości działania przedsiębiorstwa: ujęcia, stacje uzdatniania, zbiorniki, pompownie, oczyszczalnie, przepompownie, przelewy, systemy SCADA, łączność i platformy zdalnego nadzoru. Sprawdź, czy w scenariuszach awaryjnych uwzględniono utratę łączności, niedostępność SCADA, awarię platformy, brak danych z obiektów terenowych, zanik zasilania oraz ręczny tryb działania. Źródła: Dyrektywa (UE) 2022/2557, krajowe przepisy dotyczące odporności podmiotów krytycznych, własne plany ciągłości działania, scenariusze awaryjne, procedury reagowania kryzysowego, analiza krytyczności obiektów i procesów.

Regulacja / standard	Znaczenie dla wod-kan i co konkretnie sprawdzić
Dyrektywa (UE) 2020/2184 w sprawie jakości wody pitnej	Status: prawnie obligatoryjne w zakresie jakości i bezpieczeństwa wody przeznaczonej do spożycia. O co chodzi: jakość i bezpieczeństwo wody przeznaczonej do spożycia, podejście oparte na ryzyku, monitoring i dostęp do wody. Znaczenie dla wod-kan: dyrektywa nie wymaga stosowania konkretnego systemu telemetrycznego, ale wzmacnia znaczenie podejścia opartego na ryzyku, monitoringu, wiarygodności danych i doku-mentowania działań związanych z bezpieczeństwem oraz dostępnością wody. Telemetria może wspierać nadzór nad infrastrukturą, alarmowanie, analizę zdarzeń i utrzymanie ciągłości dostaw, jeżeli dane z systemu są wykorzystywane w eksploatacji lub zarządzaniu ryzykiem. Sprawdź: czy dane z telemetrii wspierają nadzór nad obiektami istotnymi dla jakości i dostępności wody: ujęciami, stacjami uzdatniania, zbiornikami, pompowniami, siecią dystrybucyjną i punktami pomiarowymi. Sprawdź, czy system pozwala wykrywać odchylenia, alarmować o zdarzeniach, odtworzyć historię parametrów i udokumentować reakcję na awarię lub zdarzenie mogące wpływać na dostawy wody. Pamiętaj, że telemetria nie zastępuje badań jakości wody ani wymagań sanitarnych, ale może wspierać nadzór operacyjny. Źródła: Dyrektywa (UE) 2020/2184, krajowe przepisy dotyczące jakości wody przeznaczonej do spożycia, wymagania Państwowej Inspekcji Sanitarnej, procedury wewnętrzne przedsiębiorstwa, dokumentacja systemu monitoringu i alarmowania.
Dyrektywa (UE) 2024/3019 – tzw. ściekowa	Status: prawnie obligatoryjne w zakresie gospodarki ściekowej i ochrony środowiska. O co chodzi: oczyszczanie ścieków komunalnych, monitoring, raportowanie i modernizacja infrastruktury ściekowej. Znaczenie dla wod-kan: dyrektywa nie nakazuje stosowania konkretnego systemu telemetrycznego, ale wzmacnia znaczenie monitoringu, raportowania i nadzoru nad infrastrukturą ściekową. Telemetria może wspierać kontrolę pracy pompowni, oczyszczalni, przepływów, przelewów, awarii i zdarzeń eksploatacyjnych oraz pomagać w dokumentowaniu reakcji na zdarzenia. Sprawdź: czy system telemetryczny obejmuje obiekty i procesy istotne dla gospodarki ściekowej: przepompownie, oczyszczalnie, przepływy, poziomy, przelewy, rzuty, awarie pomp, przeciążenia, zaniki zasilania i zdarzenia środowiskowe. Sprawdź, czy system pozwala rejestrować alarm, czas reakcji, czas usunięcia awarii i historię pracy urządzeń. Sprawdź, czy dane z telemetrii mogą wspierać raportowanie, analizę zdarzeń oraz dokumentowanie działań eksploatacyjnych. Źródła: Dyrektywa (UE) 2024/3019, Prawo wodne, pozwolenia wodnoprawne, wymagania dotyczące monitoringu i raportowania, dokumentacja oczyszczalni i przepompowni, procedury eksploatacyjne przedsiębiorstwa.
ISO/IEC 27001	Status: fakultatywne / dobra praktyka. O co chodzi: System Zarządzania Bezpieczeństwem Informacji. Znaczenie dla wod-kan: ISO/IEC 27001 nie potwierdza automatycznie bezpieczeństwa konkretnego produktu, ale może pomagać w ocenie dojrzałości organizacyjnej dostawcy, producenta, operatora usługi lub podmiotu przetwarzającego dane. Przy ocenie warto sprawdzić nie tylko sam certyfikat, ale także jego aktualność i zakres, zwłaszcza czy obejmuje obszary związane z oferowanym rozwiązaniem. Sprawdź: czy dostawca, producent, operator platformy lub podmiot przetwarzający dane posiada aktualny certyfikat ISO/IEC 27001 i jaki jest jego zakres. Sprawdź, czy certyfikat obejmuje obszary związane z oferowanym rozwiązaniem, np. projektowanie, rozwój, produkcję, sprzedaż, serwis urządzeń telemetrycznych, utrzymanie platformy, przetwarzanie danych lub zdalne wsparcie. Nie traktuj certyfikatu jako potwierdzenia bezpieczeństwa konkretnego produktu, tylko jako element oceny dojrzałości organizacyjnej dostawcy. Źródła: certyfikat ISO/IEC 27001 dostawcy, zakres certyfikacji, jednostka certyfikująca, opis usług objętych certyfikacją.
ISO 22301	Status: fakultatywne / dobra praktyka. O co chodzi: system zarządzania ciągłością działania. Znaczenie dla wod-kan: ISO 22301 nie jest wymogiem dla każdego systemu, ale może być przydatnym punktem odniesienia dla scenariuszy awaryjnych, kopii zapasowych, odtwarzania, utrzymania usług i odporności organizacyjnej. Jest szczególnie istotna tam, gdzie niedostępność telemetrii, SCADA lub platformy zdalnego nadzoru może wpływać na ciągłość działania przedsiębiorstwa.

Regulacja / standard	Znaczenie dla wod-kan i co konkretnie sprawdzić
ISO 22301 cd.	Sprawdź: czy przedsiębiorstwo posiada scenariusze awaryjne dla utraty telemetrii, SCADA, platformy zdalnego nadzoru, łączności, zasilania lub danych z obiektu. Sprawdź, czy określono dopuszczalny czas niedostępności, sposób odtworzenia, osoby odpowiedzialne, tryb pracy ręcznej oraz testy odtwarzania. Sprawdź, czy wykonywane są kopie zapasowe konfiguracji i danych oraz czy odtworzenie było kiedykolwiek testowane. Źródła: norma ISO 22301, analiza wpływu na działalność, plan ciągłości działania, procedury odtwarzania, scenariusze awaryjne, wyniki testów odtworzeniowych, dokumentacja wykonywania kopii zapasowych.
RED-DA / EN 18031	Status: prawnie obligatoryjne warunkowo, zależnie od rodzaju urządzenia, jego funkcji, technologii komunikacyjnej i sposobu wprowadzenia na rynek. O co chodzi: wymagania dotyczące urządzeń wykorzystujących komunikację radiową lub komórkową, w tym dokumentacja techniczna, deklaracja zgodności UE, funkcje komunikacyjne oraz odpowiedzialność producenta za urządzenie. Znaczenie dla wod-kan: przy urządzeniach telemetrycznych korzystających z komunikacji radiowej lub komórkowej warto sprawdzić deklarację zgodności UE, dokumentację producenta, przeznaczenie urządzenia, zakres funkcji komunikacyjnych oraz wymagania właściwe dla danej kategorii produktu. RED-DA / EN 18031 mogą mieć znaczenie w określonych przypadkach, ale należy je analizować w zakresie, w jakim mają zastosowanie do konkretnego urządzenia i jego funkcji. Sprawdź: czy urządzenie posiada deklarację zgodności UE z uwzględnieniem tego zakresu. Źródła: dyrektywa RED, deklaracja zgodności UE, dokumentacja techniczna producenta, właściwe akty i normy produktowe dla danej kategorii urządzenia.
IEC 62443	Status: fakultatywne / dobra praktyka. O co chodzi: dobre praktyki bezpieczeństwa dla systemów automatyki przemysłowej i OT, w tym podział na strefy, kanały komunikacyjne, role stron, wymagania dla systemów i komponentów. Znaczenie dla wod-kan: IEC 62443 może być użytecznym punktem odniesienia przy projektowaniu, modernizacji i ocenie telemetrii, SCADA, zdalnego dostępu oraz integracji IT/OT. Pomaga porządkować architekturę, segmentację, odpowiedzialność integratora i producenta oraz wymagania wobec urządzeń i komunikacji. Sprawdź: czy architektura telemetrii i SCADA jest opisana, czy wskazano połączenia między systemami, dostęp zdalny, role użytkowników, segmentację, ograniczenie ekspozycji urządzeń oraz zasady komunikacji tylko tam, gdzie jest potrzebna. Źródła: seria IEC 62443, dokumentacja projektowa OT, schemat architektury systemu, zasady segmentacji i dostępu zdalnego.
Data Act – Rozporządzenie (UE) 2023/2854	Status: prawnie obligatoryjne warunkowo, jeżeli produkt, usługa lub model przetwarzania danych są objęte zakresem regulacji. O co chodzi: dostęp do danych z produktów połączonych i wybranych usług cyfrowych związanych z ich działaniem, udostępnianie i eksport danych. Znaczenie dla wod-kan: Data Act nie jest regulacją cyberbezpieczeństwa, ale może mieć znaczenie przy usługach telemetrycznych, platformach danych, usługach chmurowych i zakończeniu korzystania z usługi. W projektach wod-kan warto zwracać uwagę na dostęp do danych, eksport danych, zasady korzystania z danych oraz możliwość ich przeniesienia, jeżeli dane telemetryczne są istotne dla eksploatacji, raportowania lub ciągłości działania. Sprawdź: czy w przypadku platformy danych, usługi chmurowej lub usługi cyfrowej wiadomo, kto ma dostęp do danych, w jakim zakresie i na jakich zasadach. Sprawdź, czy możesz wyeksportować dane, w jakim formacie, w jakim czasie i co dzieje się z danymi po zakończeniu korzystania z usługi. Sprawdź, czy umowa albo regulamin usługi opisują dostęp do danych, przenoszalność, eksport, retencję i zakończenie współpracy. Źródła: Rozporządzenie (UE) 2023/2854, umowa z dostawcą, regulamin platformy, dokumentacja eksportu danych, polityka retencji danych, warunki zakończenia korzystania z usługi.

Regulacja / standard	Znaczenie dla wod-kan i co konkretnie sprawdzić
AI Act – Rozporządzenie (UE) 2024/1689	Status: prawnie obligatoryjne warunkowo, jeżeli rozwiązanie wykorzystuje system AI objęty regulacją. O co chodzi: systemy sztucznej inteligencji, klasyfikacja ryzyka, obowiązki dostawców i użytkowników systemów AI. Znaczenie dla wod-kan: AI Act nie dotyczy typowej telemetrii jako takiej, ale może mieć znaczenie przy rozwiązaniach wykorzystujących uczenie maszynowe, predykcję awarii, detekcję wycieków, analizę anomalii lub automatyczne wspomaganie decyzji. W takich przypadkach warto sprawdzić rolę dostawcy, sposób działania systemu, dokumentację, dane wykorzystywane do analizy oraz zakres odpowiedzialności za wyniki generowane przez system. Sprawdź: czy rozwiązanie faktycznie wykorzystuje system AI, czy tylko klasyczną analizę danych, alarmy lub reguły. Jeżeli wykorzystywana jest sztuczna inteligencja, sprawdź do czego służy: predykcji awarii, detekcji wycieków, analizy anomalii, klasyfikacji zdarzeń albo wspomagania decyzji. Sprawdź rolę dostawcy i użytkownika, dokumentację modelu, źródła danych, sposób walidacji, nadzór człowieka, ograniczenia odpowiedzialności i sposób postępowania przy błędnych wskazaniach. Źródła: Rozporządzenie (UE) 2024/1689, dokumentacja dostawcy systemu AI, dokumentacja modelu, opis danych wykorzystywanych do analizy, procedury walidacji, zasady nadzoru człowieka i monitorowania działania systemu.

Opracowanie: Inventia Sp. z o.o.
© 2026 Inventia Sp. z o.o. Wszelkie prawa zastrzeżone.
Niniejszy materiał ma charakter informacyjny i pomocniczy. Nie stanowi opinii prawnej, audytu bezpieczeństwa, dokumentacji projektowej ani instrukcji zapewnienia zgodności z regulacjami. Jego celem jest wskazanie, gdzie szukać źródeł wiedzy o regulacjach i standardach, które mogą mieć znaczenie przy projektowaniu, zakupie, wdrażaniu i utrzymaniu systemów telemetrycznych w przedsiębiorstwach wodociągowo-kanalizacyjnych.



MODUŁ TELEMETRYCZNY	MT–025 v3	MT–058	MT–121	MT–151 LED v3	MT–151 HMI v3
Technologia			CODESYS®	CODESYS®	CODESYS®
4G (LTE)	LTE Cat 1, LTE Cat. M1/NB-IoT	LTE Cat M1 Cat-NB1/NB2	Cat 1	Cat 1	Cat 1
3G	–	–	TAK	TAK	TAK
2G	TAK	–	TAK	TAK	TAK
LoRa®	–	–	–	–	–
BLE	–	–	–	–	–
GPS	–	TAK²	–	–	–
Ethernet	–	–	TAK	10/100	10/100
SMS	TAK	–	TAK	TAK	TAK
Zasoby					
Wymiary (dł. x szer.x wys.) w mm	70x86x58	151x80x60	105x86x58	157x86x58	157x86x58
Wejścia binarne	0 – 4¹	0 – 5	8 – 16¹	16 – 28¹	16 – 28¹
Wyjścia binarne	4	–	0 – 8¹	0 – 12¹	0 – 12¹
Wejścia licznikowe	0 – 4¹	0 – 2¹	0 – 4¹	0 – 4¹	0 – 4¹
Wejścia analogowe	2	1	3	6	6
Wyjścia analogowe	–	–	1		
Wejścia 1–Wire	–	1	–	–	–
Wewnętrzny pomiar T/H	–	T/H zew. zinteg.	T	T	T
Porty Ethernet	–	–	1	1	1
Porty szeregowo RS232/422/485/TTL	1 (0/0/1/0)²	–	1 (1/0/1/0)	2 (2/0/1/0)²	2 (2/0/1/0)²
Interfejs M–Bus	–	–	–	–	–
Kanał głosowy	–	–	–	–	–
Sygnalizacja LED/wyświetlacz	TAK/–	TAK/–	TAK	TAK/–	TAK/TAK
Zegar czasu rzeczywistego (RTC)	TAK	TAK	TAK	TAK	TAK
Rozłączalne listwy zaciskowe	TAK	TAK	TAK	TAK	TAK
Złącze anteny GSM	1 x SMA	1 x SMA	1 x SMA	1xSMA	1xSMA
Antena GPS	–	–	–	–	–
Obsługa kart SIM	SIM/MIM²	SIM/MIM²	SIM/MIM²	2xSIM/MIM²	2xSIM/MIM²
Sposób mocowania	szyna DIN	powierzchniowy	szyna DIN	szyna DIN	szyna DIN
Obudowa	ABS	ABS/PC UL 94 V0²	ABS	ABS	ABS
Napięcie zasilania	9,5–30 V DC	7–24	10,8–30	10,8–30	10,8–30
Zasilanie czujników zewnętrznych)	–	5	–	–	–
Wewnętrzna bateria zasilająca	–	3xR14 (4,5V) lub 3,6V/D²	–	–	–
Akumulator wew./zew.	– /–	–	–	–/TAK	–/TAK
Temperatura pracy (°C)	-20 ... +55	-20 ... +60	-20 ... +55	-20...+65	-20...+65
Klasa ochrony	IP20	IP68	IP20	IP20	IP20
Funkcjonalność					
Wysyłanie/Odbieranie SMS	TAK	–	–	TAK	TAK
Wysyłanie SMS do grup odbiorców	TAK	–	–	–	–
Konfiguracja przez SMS	TAK	–	–	–	–
WebGUI	–	–	–	–	–
Wysyłanie pakietów danych	TAK	TAK	TAK	TAK	TAK
Praca zdarzeniowa	TAK	TAK	TAK	TAK	TAK
Program Użytkownika (maks. ilość linii)	–	–	TAK	TAK	TAK
Modbus RTU (master/slave)	–	–	TAK/TAK	TAK/TAK	TAK/TAK
Modbus TCP (client/server)	–	–	TAK/TAK	TAK/TAK	TAK/TAK
Klient MQTT	TAK	TAK	–	–	–
Open/Open2	TAK/–	TAK/–	TAK/TAK	TAK/TAK	TAK/TAK
Format ramki UDP Standard	–	–	TAK	TAK	TAK
Praca w trybie niskiego poboru energii	–	TAK	–	–	–
Rejestrator	TAK	TAK	TAK	TAK	TAK
Obsługa przez MT Data Provider	TAK	TAK	TAK	TAK	TAK
NTP	Klient	Klient	Klient	Klient	Klient
Zdalna aktualizacja oprogramowania	TAK	TAK	TAK	TAK	TAK
Zdalna konfiguracja	TAK	TAK	TAK	TAK	TAK



1/ ilość wejść/wyjść binarnych i licznikowych jest konfigurowalna
2/ opcja
3/ lub -20 ... 55°C - zależnie od wersji wewnętrznej akumulatora

MODUŁ TELEMETRYCZNY	MT–221	MT–718 PS	MTX-2050 v4	EX-A41	EX-D16
Technologia	CODESYS®				
4G (LTE)	Cat 1	LTE Cat 1, LTE Cat. M1/NB-IoT	Cat 1	–	–
3G	TAK	–	–	–	–
2G	TAK	TAK	TAK	–	–
LoRa®	–	–	–	–	–
BLE	–	TAK²	–	–	–
GPS	–	zew. GPS NMEA²	–	–	–
Ethernet	TAK	–	10/100	TAK	TAK
SMS	TAK	TAK	TAK	–	–
Zasoby					
Wymiary (dł. x szer.x wys.) w mm	105x86x58	203x125x90	105x86x59	52,5x86x58	52,5x86x58
Wejścia binarne	–	0 – 5	0 – 4¹	–	8 – 16¹
Wyjścia binarne	–	2	0 – 2¹	–	0 – 8¹
Wejścia licznikowe	–	0 – 5¹	0 – 4¹	–	–
Wejścia analogowe	–	2	–	4	–
Wyjścia analogowe	–	–	–	1	–
Wejścia 1–Wire	–	–	–	–	–
Wewnętrzny pomiar T/H	T	T/H²	T	–	–
porty Ethernet	1	-	1	1	1
Porty szeregowo RS232/422/485/TTL	1 (1/0/1/0)	1 (0/0/1/0)²	2 (1/0/2/0)²	1 (0/0/1/0)	1 (0/0/1/0)
Interfejs M–Bus	–	–	1	–	–
Kanał głosowy	–	–	–	–	–
Sygnalizacja LED/wyświetlacz	TAK	TAK/–	TAK/–	TAK/–	TAK/–
Zegar czasu rzeczywistego (RTC)	TAK	TAK	TAK	TAK	TAK
Rozłączalne listwy zaciskowe	TAK	TAK	TAK	TAK	TAK
Złącze anteny GSM	1 x SMA	1 x SMA	2 x SMA	–	–
Antena GPS	–	–	–	–	–
Obsługa kart SIM	SIM/MIM²	SIM/MIM²	2xSIM/MIM²	–	–
Sposób mocowania	szyna DIN	powierzchniowy	szyna DIN	szyna DIN	szyna DIN
Obudowa	ABS	PC UL94V-0	ABS	ABS	ABS
Napięcie zasilania	10,8–30 V DC	PC UL94V-0	10,8–53 V DC	12/24 V DC	12/24 V DC
Zasilanie czujników zewnętrznych)	–	0 - 5/15²/24² V DC	–	–	–
Wewnętrzna bateria zasilająca	–	6XR20	–	–	–
Akumulator wew./zew.	–	– /–	– /–	–	–
Temperatura pracy (°C)	-20 ... +65	-20 ... +55	-30 ... +65	-25 ... +55	-25 ... +55
Klasa ochrony	IP20	IP68	IP20	IP20	IP20
Funkcjonalność					
Wysyłanie/Odbieranie SMS	TAK	TAK	TAK	–	-
Wysyłanie SMS do grup odbiorców	–	–	TAK	–	-
Konfiguracja przez SMS	–	TAK	–	–	-
WebGUI	–	–	TAK	–	-
Wysyłanie pakietów danych	TAK	TAK	TAK	TAK	TAK
Praca zdarzeniowa	TAK	TAK	TAK	–	–
Program Użytkownika (maks. ilość linii)	TAK	μProg (32 lines)	–	–	–
Modbus RTU (master/slave)	TAK/TAK	TAK/–	TAK/TAK	– /TAK	– /TAK
Modbus TCP (client/server)	TAK/TAK	–	TAK/TAK	– /TAK	– /TAK
Klient MQTT	–	–	–	–	–
Open/Open2	TAK/TAK	TAK /TAK	– /–	–	–
Format ramki UDP Standard	TAK	–	–	–	–
Praca w trybie niskiego poboru energii	–	TAK	–	–	–
Rejestrator	TAK	TAK	TAK	–	–
Obsługa przez MT Data Provider	TAK	TAK	TAK	TAK	TAK
NTP	Klient	–	Klient	–	–
Zdalna aktualizacja oprogramowania	TAK	TAK	TAK	TAK	TAK
Zdalna konfiguracja	TAK	TAK	TAK	TAK	TAK

1/ ilość wejść/wyjść binarnych i licznikowych jest konfigurowalna
2/ opcja
3/ lub -20 ... 55°C - zależnie od wersji wewnętrznej akumulatora

DLACZEGO INVENTIA?



KOMPLEKSOWE ROZWIĄZANIE END-TO-END

Od urządzeń w terenie po dane w Twoich rękach



URZĄDZENIA W TERENIE TRANSMISJA DANYCH OPROGRAMOWANIE I DANE WSPARCIE I ROZWÓJ

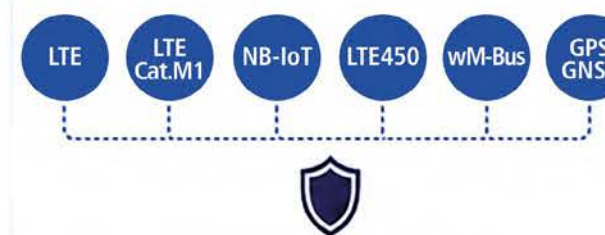
SKALOWALNOŚĆ BEZ OGRANICZEŃ

Od małych instalacji po setki lokalizacji



ELASTYCZNOŚĆ I NIEZAWODNOŚĆ

Wiele technologii - jeden cel



AUTOMATYCZNE PRZEŁĄCZANIE I ZAPEWNIENIE CIĄGŁOŚCI DANYCH

DOPASOWANIE DO WIELU BRANŻ

Rozwiązania dla kluczowych sektorów



PEŁNA KONTROLA I WGLĄD W DANE



WYŻSZA EFEKTYWNOŚĆ I NIŻSZE KOSZTY



BEZPIECZEŃSTWO I NIEZAWODNOŚĆ



LEPSZE ZARZĄDZANIE I ZRÓWNOWAŻONY ROZWÓJ

Ofertę Inventii wyróżnia:



- Wysoki poziom cyberbezpieczeństwa**, potwierdzony zgodnością z normą **ISO/IEC 27001**, obejmujący **szyfrowanie transmisji danych algorytmem AES-128, zarządzanie dostępem do danych, konfiguracji oraz programu na urządzeniach Inventii, a także aktualizacji oprogramowania**
- Możliwość zdalnej konfiguracji, programowania logiki sterowania i aktualizacji firmware'u** w zainstalowanych urządzeniach poprzez 2G/4G (Cat. 1, Cat. M1, NB-IoT, LTE450)
- Elastyczność systemu**, dzięki wykorzystaniu otwartych standardów (**MQTT, Modbus TCP, Modbus RTU**)
- Możliwość współpracy z zewnętrznymi urządzeniami (sterowniki PLC, układy wejść/wyjść, urządzenia pomiarowe)**, obsługującymi standardowe protokoły komunikacyjne (**np. Modbus RTU/TCP, Gazmodem, M-BUS, NMEA, Genibus, IEC 60870-5-140**)
- Możliwość korzystania z **dowolnego systemu wizualizacji**, dzięki udostępnianiu danych poprzez **standardowy interfejs OPC (OPC DA, OPC UA)**
- Łatwość integracji z bazami danych i środowiskiem informatycznym Użytkownika**, dzięki udostępnieniu danych przy pomocy **interfejsu ODBC i plików CSV**
- Minimalne koszty użytkowania** (zdalne zarządzanie i aktualizacje, transmisja spontaniczna inicjowana zdarzeniami, tworzenie zwierciadła stanu urządzeń zewnętrznych, zaawansowana diagnostyka, skalowalność)
- Możliwość **integracji w jednym, spójnym systemie** różnych urządzeń telemetrycznych, w dwóch wariantach: **w chmurze DataPortal lub samodzielnym rozwiązaniu uruchamianym na maszynie Klienta – MTDataProvider**
- Polski producent z pełnym wsparciem technicznym i serwisem realizowanym w kraju**. Dzięki własnemu działowi **R&D** firma Inventia oferuje **rozwiązania pod klucz**, a także **realizację projektów OEM oraz dostosowanie sprzętu i oprogramowania do specyficznych wymagań Klienta**, zarówno w warstwie sprzętowej, jak i systemowej

Inventia to polska firma technologiczna, która od 25 lat dostarcza zaawansowane rozwiązania telemetryczne i systemy IoT, stanowiąc fundament cyfryzacji infrastruktury rozproszonej, ze szczególnym uwzględnieniem sektora wodociągowo-kanalizacyjnego. Jako lider rynku, firma oferuje szeroką gamę modułów telemetrycznych (RTU), sterowników PLC oraz energooszczędnych rejestratorów danych zasilanych bateryjnie (moduły MT-718 i MT-058), dedykowanych do pracy w trudnych warunkach środowiskowych. Urządzenia te wspierają nowoczesne standardy komunikacji mobilnej, w tym LTE Cat. M1, NB-IoT oraz dedykowane pasmo LTE450, co zapewnia stabilność transmisji nawet w trudno dostępnych lokalizacjach. W branży wod-kan rozwiązania Inventii są kluczowe dla monitorowania przepływów i ciśnień, kontroli i zdalnego nadzoru nad przepompowniami ścieków, stacjami uzdatniania wody oraz wykrywania awarii i wycieków w czasie rzeczywistym.

W odpowiedzi na wymogi dyrektywy NIS2, Inventia kładzie szczególny nacisk na cyberbezpieczeństwo sieci telemetrycznych i systemów nadzoru nad obiektami (OT). Produkty firmy zapewniają szyfrowaną transmisję danych i rygorystyczną kontrolę dostępu do urządzeń, chroniąc integralność infrastruktury krytycznej. Atutem Inventii jest połączenie doświadczenia technologicznego z potwierdzonymi standardami jakości i bezpieczeństwa informacji, czego dowodem są certyfikaty ISO 9001 oraz ISO/IEC 27001. Ofertę uzupełnia profesjonalne doradztwo techniczne, wsparcie projektowe oraz szkolenia dla integratorów i użytkowników, ułatwiające budowę odpornych i optymalnych kosztowo systemów zarządzania zasobami wodnymi w Polsce i na świecie.



INVENTIA Sp. z o.o.
Poleczki 23, 02-822 Warszawa
tel.: +48 22 545 32 00
BOK: +48 22 545 32 30
www: inventia.pl, coolsens.eu,
agreus.pl, dataportal.pl, xway.pl
inventia@inventia.pl
info@inventia.pl



inventia.pl



Obserwuj nas na LinkedIn

Ekosystem telemetryczny Inventii dedykowany infrastrukturze krytycznej

