



wersja 2.8

### Kamery

IBH-11, IBH-21, IBH-31, ICH-22, ICH-32, ICH-42, IFH-31IR, IFH-42IR, IFH-61IR, IMH-22, IMH-10N, IDH-11IR, IDH-21IR, IDH-21IRF, IDH-21IRF2, IDH-31IR, IDH-41IR, IDH-41IRKL, IDH-42IRL, IDH-32XR, IDH-42XR, IDH-42XRKL, IDH-84IR, IDH-23VR, IDH-23MR, IDH-33VR, IDH-43MR, IDH-43MRL, IDH-84MR, IWH-11IR, IWH-21IR, IWH-21IRF, IWH-23IRF, IWH-22IRL, IWH-21IRF, IWH-31IR, IWH-41IR, IWH-41IRKL, IWH-42IRL, IWH-32XR, IWH-43XR, IWH-84IR, IWH-23VR, IWH-23MR, IWH-33VR, IWH-43MR, IWH-43MRL, IWH-84MR, SIBH-2020, SICH-2020, SICH-2020R, SICH-2030, SICH-2030R, SICH-2025RK, SICH-2036AUT, SIMH-2004, SIMH-2004R, SINH-2004L, IDH-23PTZ

### Pozbywanie się starych urządzeń elektrycznych

To urządzenie jest oznaczone zgodnie z Ustawą o zużytych sprzęcie elektrycznym i elektronicznym symbolem przekreślonego kontenera na odpady. Takie oznakowanie informuje, że sprzęt ten, po okresie jego użytkowania nie może być umieszczany łącznie z innymi odpadami pochodzącymi z gospodarstwa domowego. Użytkownik jest zobowiązany do oddania go prowadzącym zbieranie zużytego sprzętu elektrycznego i elektronicznego. Prowadzący zbieranie, w tym lokalne punkty zbiórki, sklepy oraz gminne jednostki, tworzą odpowiedni system umożliwiający oddanie tego sprzętu. Właściwe postępowanie ze zużytym sprzętem elektrycznym i elektronicznym przyczynia się do uniknięcia szkodliwych dla zdrowia ludzi i środowiska naturalnego konsekwencji, wynikających z obecności składników niebezpiecznych oraz niewłaściwego składowania i przetwarzania takiego sprzętu.



### Warunki eksploatacyjne

- Nie należy narażać kamery na gwałtowne ruchy lub drgania
- Przed podłączeniem zasilania sprawdzić poprawność napięcia i polaryzacji zasilania
- Nieprawidłowe zasilanie może być powodem pożaru lub porażenia prądem elektrycznym
- Należy zawsze używać kamerę w miejscu dobrze wentylowanym, aby uniknąć jej przegrzania
- Warunki eksploatacji: Temperatura oraz wilgotność zgodnie z danymi stosowanej kamery

### Ważne ostrzeżenia

- Urządzenie musi być zasilane zgodnie z wytycznymi podanymi w instrukcji lub danych technicznych. Nieprawidłowe zasilanie może być powodem pożaru lub porażenia prądem elektrycznym
- Nie wolno narażać urządzenia na wilgoć oraz kontakt z wodą albo innymi cieczami. Może to powodować pożar, porażenie prądem elektrycznym albo może uszkodzić urządzenie
- Nie wolno kłaść ciężkim przedmiotów na obudowie albo kablu zasilającym. Uszkodzenie kabla zasilającego może spowodować pożar albo porażenie prądem elektrycznym
- Nie wolno kłaść pojemników z cieczami albo małymi obiektami metalowymi na obudowie. W przypadku dostania się do wnętrza urządzenia ciecze albo małe metalowe objekty mogą spowodować pożar albo porażenie prądem elektrycznym
- Nie wolno nacinać, łamać, skręcać, ciągnąć lub nagrzewać przewód zasilający. Uszkodzenie kabla zasilającego może spowodować pożar albo porażenie prądem elektrycznym
- Nie demontować obudowy. Jej demontaż może skutkować porażeniem elektrycznym. Wszelkie prace serwisowe należy zlecić przeszkolonemu i autoryzowanemu serwisowi.
- Nie wolno w żaden sposób modyfikować urządzenia. Może to spowodować pożar albo porażenie prądem elektrycznym

- W przypadku burzy należy natychmiast wyłączyć zasilanie i wyjąć kabel zasilający z gniazda. Uszkodzenia spowodowane wyładowaniami atmosferycznymi mogą spowodować pożar albo porażenie prądem elektrycznym
- W przypadku dymu, wyczuwalnego zapachu lub szumu (włączając nadmierny szum wentylatora) należy natychmiast wyłączyć zasilanie i wyjąć przewód zasilający z gniazda. Dalsze użytkowanie urządzenia może spowodować pożar albo porażenie prądem elektrycznym. Wymagana jest interwencja serwisowa przeszkolonego i autoryzowanego serwisu
- Jeżeli urządzenie upadło albo zostało uszkodzone należy natychmiast wyłączyć zasilanie i wyjąć przewód zasilający z gniazda. Dalsze użytkowanie urządzenia może spowodować pożar albo porażenie prądem elektrycznym. Wymagana jest interwencja serwisowa przeszkolonego i autoryzowanego serwisu
- Nie wolno dotykać urządzenia mokrymi rękoma. Może to spowodować porażenie prądem elektrycznym
- Należy przestrzegać prawidłowej kolejności podłączania urządzeń – najpierw połączenia sygnałowe, a na końcu zasilające. Zasilanie urządzeń włączamy dopiero po podłączeniu wszystkich kabli. Nie stosowanie się to tego zalecenia może spowodować porażenie prądem elektrycznym lub uszkodzenie urządzeń
- Nie wolno używać lub przechowywać urządzenia w następujących warunkach:
  - miejsca zbyt zimne lub ciepłe
  - o zbyt dużej wilgotności powietrza
  - obszary o zbyt dużym zapyleniu
  - miejsca gdzie nie jest możliwa wentylacja urządzenia przez wszystkie szczeliny
- Nie należy zbliżać do urządzenia lub kłaść na nim kart bankomatowych, telefonicznych, biletów albo innych magnetycznych nośników danych
- Ładunki elektrostatyczne mogą uszkodzić urządzenie. Należy usunąć ładunki elektrostatyczne z ciała przed dotknięciem panela tylnego ze złączami albo części elektronicznych wewnątrz urządzenia
- W przypadku kiedy urządzenia nie można naprawić lub jest zastępowane przez inne należy je utylizować zgodnie z lokalnym prawem
- Urządzenie zapisuje dane na dysku. Awaria lub usterka w pracy kamery i/lub dysku może spowodować utratę lub uszkodzenie danych albo uniemożliwić zapis nagrań. Utrata danych, w tym nagrań, nie podlega gwarancji oraz odpowiedzialności producenta, importera oraz dystrybutora urządzenia
- Urządzenie umożliwia zmianę parametrów pracy przez użytkownika. Oznacza to że błąd w konfiguracji spowodowany przez użytkownika może spowodować nieprawidłowe działanie urządzenia, w tym zaprzestanie rejestracji. Urządzenie powinno być instalowane i konfigurowane przez przeszkoloną osobę
- Jeżeli urządzenie jest połączone z innymi urządzeniami (np. kamery, czujniki, sieć komputerowa, dyski twarde itp.) zawsze istnieje możliwość uszkodzenia spowodowana przyczynami zewnętrznymi. Należy zapewnić przeglądy okresowe.

Importer i dystrybutor:  
GDE POLSKA  
Włosań, ul. Świątnicka 88  
32-031 Mogilany  
www.gde.pl

Wszelkie uwagi i poprawki prosimy zgłaszać na adres:  
[cctv@gde.pl](mailto:cctv@gde.pl)

Ze względu na doskonalenie urządzeń i oprogramowania możliwe jest pojawienie się nowych funkcji nieujętych w niniejszej instrukcji.

**Najnowszą wersją tej instrukcji oraz jej pełna wersja znajduje się na stronie [http://www.gde.pl/Do\\_pobrania/](http://www.gde.pl/Do_pobrania/) - dział MAZi Security, również tam znajdziemy oprogramowanie, firmware'y oraz inne przydatne dane.**

## 1. Podłączenie kamery

LAN port Ethernet (wtyk RJ-45) – port sieciowy oraz zasilania PoE IEEE 802.3af (kamery stacjonarne).

Zasilanie 12V DC (kamery stacjonarne) / 24 V AC (kamery obrotowe).

Podłączając zasilanie należy zwrócić uwagę na prawidłową polaryzację zasilania.

Nie wolno zasilac kamer równocześnie przez złącza zasilania oraz port LAN – PoE.

W zależności od wersji kamery mogą posiadać dodatkowe złącza np. dla kart mikro SD lub wejścia i wyjścia alarmowe.

Po podłączeniu sieci LAN oraz zasilania logujemy się do kamery.

Możliwy jest wybór języka – np. polskiego.

## 2. Domyślne ustawienia kamery

**adres IP:** 192.0.0.64 (menu niebieskie, firmware nie wymaga aktywacji) albo 192.168.1.64 (menu zielone, firmware wymaga aktywacji)

W niektórych wersjach firmware'ów adres przypisywany jest dynamicznie przez serwer DHCP.

Do ustalenia adresu IP możemy użyć programu **VMS-A1** lub **SADPTool** – do pobrania z [http://www.gde.pl/Do\\_pobrania/](http://www.gde.pl/Do_pobrania/) - dział „MAZi Security (firmware'y, oprogramowanie)”.

**login:** admin

**hasło:** takie jak nadano podczas aktywacji lub 12345 lub MAZi12345 (uwaga na małe i duże litery)

**port HTTP:** 80, **port HTTPS:** 443, **port RTSP:** 554, **port SDK:** 8000

Przy udostępnieniu kamery w Internecie wszystkie powyższe pory muszą być przekierowane.

Bezwzględnie zaleca się po zakończeniu konfiguracji kamery przydzielić jej stały adres IP. Pozwoli to uniknąć jego zmiany np. po awarii zasilania, kiedy serwer DHCP ponownie przydziela adresy IP.

### Blokada logowania

W przypadku 6 nieudanych prób logowania kamera blokuje możliwość logowania z danego urządzenia na pół godziny. Rejestrator do którego podłączona jest kamera może wyświetlać komunikat błędny login lub hasło lub braku obrazu. Jeśli nie chcemy czekać można wyłączyć i włączyć kamerę, wtedy można zalogować się od razu.

Istnieje możliwość wyłączenia tej funkcji w *Konfiguracja* → *System* → *Bezpieczeństwo* → *Funkcje bezpieczeństwa* → *Włączenie blokady nieuprawnionego logowania*

## 3. Aktywacja kamery

**Kamery wyposażone w nowe firmware'y wymagają aktywacji i nie posiadają hasła fabrycznego.**

Przy pierwszym uruchomieniu należy podać hasło (zawierające minimum 8 znaków, litery oraz cyfry). Dopiero po wprowadzeniu hasła urządzenie staje się aktywne i mamy do niego pełen dostęp poprzez sieć LAN.

Aktywacja możliwa jest lokalnie z menu rejestratora, przez program **VMS-A1** w najnowszej dostępnej wersji oraz przez program **SADPTool** – dostępne na naszej stronie [www.gde.pl/do-pobrania](http://www.gde.pl/do-pobrania).

Aktywacja możliwa jest także bezpośrednio z rejestratorów m. in. INVR-xxAL, INVR-16/32A, HAVR-xxxxLT/HT i nowszych. Opcja znajdziemy w *Menu* → *Kamery* → *Kamera IP*, tam gdzie wyszukujemy i dodajemy kamery do rejestratora. W przypadku braku takiej opcji należy zaktualizować firmware w rejestratorze.

Podłączenie kamery wymagającej aktywacji do rejestratora z PoE:

- rejestratory serii AL, KL, K, Q, QL – aktywacja następuje automatycznie po podłączeniu kamery do porty PoE, użytkownik ma możliwość podglądnięcia hasła przydzielonego kamerze, standardowo jest to hasło administratora rejestratora lub specjalne hasło do aktywacji kamer ustawione podczas konfiguracji rejestratora
- rejestratory INVR-04/08POE oraz IMVR-04/08POE – aktywacji należy dokonać samodzielnie, następnie:
  - ustawić adres IP z puli wewnętrznej rejestratora, standardowo 192.168.254.2 do 9,
  - podłączyć kamerę do portu PoE w rejestratorze o numerze jak adres *IP-1*, np. 192.168.254.2 czyli podłączamy do portu 1
  - w menu *Kamera* -> *Kamera IP* -> *Edytuj* ustawiany na Sterowanie ręczne, protokół ONVIF, port 80, login i hasło
  - sprawdzamy czy mamy obraz

## 4. Połączenie zdalne

Zagadnienie zdalnego dostępu jest szczegółowo opisane w instrukcji „MAZi – zdalny dostęp przez DDNS i chmurę” dostępnej do pobrania w [http://www.gde.pl/Do\\_pobrania/](http://www.gde.pl/Do_pobrania/) – dział MAZi Security. Opisano tam dostęp przez chmurę, adres IP/domenowy/DDNS a także za pomocą przeglądarki, programu VMS-A1, Guarding Vision oraz CCTV View.

## 5. Połączenie za pomocą przeglądarki

Konfiguracja kamery oraz podgląd możliwy jest przez **Internet Explorer** (zalecana), Mozilla Firefox w wersji 52 ESR oraz Apple Safari. Przeglądarki Chrome, Opera, Edge, Firefox (powyżej wersji 52) i wiele innych nie obsługuje wymaganych wtyczek NPAPI. W systemie Windows wymagane jest zainstalowanie wtyczki WebComponents – powinno nastąpić to automatycznie w chwili pierwszego połączenia z kamerą.

W przypadku przeglądarki Chrome wymagana jest obsługa wtyczek NPAPI. Wtyczki NPAPI nie działają w Chrome w wersji 42 lub nowszej. W przypadku Chrome do wersji 45 można włączyć obsługę NPAPI.

Włączamy Chrome, na pasku adresu wpisujemy *chrome://flags/#enable-npapi*, a następnie klikamy link *Włącz interfejs NPAPI*. Teraz klikamy przycisk *Uruchom ponownie teraz*.

W przypadku systemu MacOS i przeglądarki Safari wtyczkę należy zainstalować ręcznie, można ją pobrać z [http://www.gde.pl/Do\\_pobrania/](http://www.gde.pl/Do_pobrania/) - dział Rozwiązania IP MAZi.

Łączymy się z kamerą podając adres i port HTTP np. <http://192.0.0.64:80>

### Najczęściej spotykane problemy związane z dostępem przez przeglądarkę Internet Explorer

Omyłkowe używanie przeglądarki Edge zamiast Internet Explorer spowodowane podobną ikoną.

Brak podglądu lub ciągle żądanie instalacji kontrolki:

- wejść w *Narzędzia* → *Opcje internetowe* → zakładka *Zabezpieczenia*
- wybieramy *Internet* (opcjonalnie możemy zrobić to dla *Intranetu* jeśli tam jest kamera, albo dodać ją do *Zaufanych witryn* i tam zmodyfikować ustawienia)
- klikamy w *Poziom niestandardowy*
- tylko IE9, IE10 i wyższe – *Zezwalaj na Filtrowanie ActiveX* – *wyłącz*
- wszystkie IE: *inicjowanie i wykonywanie skryptów kontrolek ActiveX niezaznaczonych jako bezpieczne do wykonywania* – *monituj*
- *pobieranie niepodpisanych kontrolek ActiveX* – *monituj*
- *pobieranie podpisanych kontrolek ActiveX* – *monituj*
- *uruchamianie kontrolek ActiveX i wtyczek* - *włącz*
- zapisz modyfikacje klikając *OK* i wyjdź z menu *Zabezpieczeń*.
- czasem może być potrzebne przeładowanie komputera a zawsze ponowne uruchomienie przeglądarki

Czasem może być konieczne dodanie rejestratora do *Widoku zgodności*. Zazwyczaj dotyczy to IE10 i wyższe.

- wejść w *Narzędzia* a następnie w *Ustawienia widoku zgodności*
- dodajemy rejestrator wpisując jego adres o ile sam się nie pojawił
- warto także zaznaczyć *Wyświetlaj witryny intranetu w widoku zgodności*
- zamykamy okno, ponownie uruchamiamy przeglądarkę

Jeśli w dalszym ciągu nie działa podgląd w albo mamy inne problemy wtedy sprawdzamy (*Narzędzia* → *Zarządzaj dodatkami*) czy następujący dodatek jest włączony: *WebVideoActiveX Control*. Przy pierwszym uruchomieniu może pojawić się monit czy uruchomić – wybieramy *Zawsze dla wszystkich witryn*.

## 6. Dostęp przez program SADPTool oraz VMS-A1

Zalecany program do zarządzania jest **SADPTool**, jego funkcje:

- aktywacja kamer
- wyszukiwanie i zmianę adresów IP wszystkich urządzeń MAZi
- odzyskiwanie hasła administratora
- sprawdzenie wersji firmware'u

**VMS-A1** to program klasy VMS, jego funkcje:

- aktywacja kamer
- wyszukiwanie i zmianę adresów IP wszystkich urządzeń MAZi
- podgląd na żywo
- przeglądanie nagrań
- konfigurację wszystkich urządzeń MAZi
- wielopoziomowa e-mapa
- praca wielomonitorowa
- tworzenie wirtualnych urządzeń składających się z wielu różnych urządzeń fizycznych

Łączymy się z kamerą podając adres IP i port SDK lub logując się do konta w chmurze.

## 7. Podłączenie za pomocą protokołu ONVIF

Protokół ONVIF wykorzystywany jest jako uniwersalny protokół do komunikacji między urządzeniami CCTV różnych producentów. W kamerach do firmware'u 5.4 jest on zawsze aktywny.

Wraz z nowymi modelami kamer wyposażonymi w firmware od wersji 5.5 wprowadzono nową funkcję zwiększającą bezpieczeństwo kamer IP. Obecnie protokół ONVIF jest fabrycznie wyłączony, co m.in. utrudnia wykrycie i połączenie z kamerą za pomocą popularnych narzędzi korzystających ze standardowego protokołu jakim jest ONVIF, a także może utrudnić uzyskanie połączenia z rejestratorem innej marki niż MAZi.

Jeśli dodajemy takie kamery do rejestratora MAZi serii INVR-xx IMVR-xx należy również włączyć protokół ONVIF i dodać kamerę ręcznie wybierając protokół MAZi-C, port zarządzania 80 z użyciem danych użytkownika ONVIF.

W tych przypadkach konieczne jest skonfigurowanie protokołu ONVIF.

W zakładce *Configuration / Konfiguracja* → *Network / Sieć* → *Advanced Settings / Ustawienia Zaawansowane* → *Integration Protocol / Protokół Integracji* zaznaczamy *Enable ONVIF*.

Następnie dodajemy użytkownika klikając a *Add / Dodaj*, następnie *Login, Hasło* i poziom uprawnień. *Media user* – posiada dostęp do podglądu on-line oraz odczytu funkcji oraz ustawień kamery (profil, DNS, interfejs sieciowy, parametry nagrywania itp.). *Operator* – dostęp to wszystkich ustawień poza możliwością zmiany kluczowych parametrów takich jak brama domyślna/adres routera, przywrócenia ustawień fabrycznych, aktualizacji oprogramowania oraz odczytu poufnych informacji takich jak logi. *Administrator* – dostęp do wszelkich funkcji bez ograniczeń.

Zarządzanie użytkownikami w protokole ONVIF jest niezależne od zarządzania użytkownikami systemowymi.

W przypadku otrzymania komunikatu błędny login lub hasło lub braku obrazu należy na chwilę wyłączyć i włączyć kamerę.

## 8. Dostęp z urządzeń mobilnych.

Kamera pozwala na zdalny monitoring za pomocą rejestratorów analogowych, rejestratorów IP, kamer IP stacjonarnych, obrotowych marki MAZi. Możliwe jest odtwarzanie nagrań, lokalne nagrywanie, wykonywanie zrzutów, sterowanie kamerami PTZ oraz wyjściami alarmowymi. Wymaga prawidłowo skonfigurowanych urządzeń sieciowych do których podłączone są urządzenia z którymi się łączymy. W przypadku braku płynności należy zmniejszyć rozdzielczość, liczbę klatek i bitrate w kamerze lub zmniejszyć jakość obrazu.

Jakość i płynność połączenia zdalnego zależy od jakości łącza sieciowego i wydajności telefonu lub tabletu.

Łączymy się z kamerą podając adres IP i port SDK lub logując się do konta w chmurze.

**Program Guarding Vision** – zalecany, aplikacja obsługująca wszystkie generacje rejestratorów, serwis Guarding Vision oraz chmurę. Guarding Vision dostępny jest na urządzenia z systemem Android jak i iOS. Można go znaleźć w Apple Store (<https://itunes.apple.com/us/app/guarding-vision/id1101697283?mt=8>) oraz w Google Play (<https://play.google.com/store/apps/details?id=com.mcu.guardingvision&hl=pl>)

## 9. Konfiguracja usługi chmura

Dzięki chmurze zdalny dostęp do kamery z przeglądarki oraz klienta mobilnego jest bardzo prosty, a co najważniejsze, pozwala na zdalny dostęp przez sieci LTE oraz 3G, gdzie tradycyjne sposoby połączenia z kamerą nie działają. Szczegóły – patrz punkt 4.

Wymagany jest program GuardingVision lub CCTV Viewer. Dostęp przez chmurę możliwy jest także z poziomu programu VMS-A1 w wersji co najmniej V2.4.0.5 build 20151026 lub przez przeglądarkę.

Dostęp przez przeglądarkę Internet Explorer (zalecana) wymaga zainstalowania wtyczki

<http://www.hicloudcam.com/assets/deps/PCPlayer.exe>.

1. Włączamy dostęp do platformy w menu *Konfiguracja* → *Sieć* → *Ustawienia zaawansowane* → *Dostęp do platformy*, w polu *Status* musi pojawić się komunikat *Online / Połączony*.
2. Może być konieczne nadanie kodu weryfikacyjnego
3. Tworzymy konto przez opcję *Register* na stronie głównej <http://www.hicloudcam.com>.
4. W czasie rejestracji podajemy adres e-mail na który zostanie wysłany mail z kodem aktywacyjnym. 4-cyfrowy kod aktywacyjny podajemy w oknie aktywacji konta w chmurze.
5. W kolejnym kroku dodajemy kamerę. Można dodać go automatycznie przez *Add Automatically* (jeśli jesteśmy w tej samej sieci LAN co kamera) albo ręcznie przez *Add by Serial No.* (jeśli jesteśmy pracujemy zdalnie) – wtedy należy podać numer seryjny kamery z naklejki na kamerze.
6. Kolejny etap to podanie kod weryfikacyjnego odczytanego z menu kamery.
7. W przypadku gdy nie ma podanego kodu weryfikacyjnego stosujemy kod standardowy *AAAAAA* lub *ABCDEF* – w pewnych przypadkach może też być wymagana aktualizacja firmware'u
8. Mając dodaną kamerę przez *Video Library* wybieramy kamery do podglądu.

W przypadku przeglądarki oraz programów na urządzenia mobilne dostęp do kamery jest możliwy po zalogowaniu się wcześniej utworzone konto.

Należy pamiętać że jest niezbędne prawidłowe skonfigurowanie ustawień sieciowych w kamerze, lecz nie potrzebujemy przekierowania portów na routerze.

W przypadku gdy podczas dodawania kamery do konta w chmurze pojawi się komunikat *Incorrect verification code / Błędny kod weryfikacyjny* należy zaktualizować firmware w kamerze – wymagany może być kontakt z działem CCTV firmy GDE Polska.

## 10. Wymagania by zdalny dostęp do kamery był możliwy

- prawidłowo wpisane adres kamery, adresy serwerów DNS oraz adres routera
- brak blokowania połączeń przychodzących przez dostawcę internetu
- w przypadku połączenia przez chmurę konfiguracja routera jak poniżej jest niepotrzebna
- przekierowane w routerze porty HTTP, HTTPS, RTSP oraz SDK
- prawidłowo skonfigurowany firewall w routerze
- wyłączona usługa UPnP na routerze jak i w kamerze o ile nie korzystamy z niej świadomie. Wyłączenie UPnP w kamerze dokonujemy w *Konfiguracja* → *Konfiguracja Zaawansowana* → *Sieć* → *UPnP* → odznaczyć *Enable UPnP*
- wyłączona funkcja DMZ w routerze
- router musi posiadać routowalny (zewnętrzny) stały lub dynamiczny adres IP
- jako DDNS można wykorzystać serwis MAZi DDNS dostępny bezpłatnie dla urządzeń MAZi

## 11. Sugerowane wartości strumieni w kamerach

Sugerowane wartości strumienia z kamer w Mb/s

Liczba klatek

Rozdzielczość	H.264			H.265		
	25 kl/s	15 kl/s	8 kl/s	25 kl/s	15 kl/s	8 kl/s
VGA 640x480	1,0	0,5	0,4	0,7	0,3	0,2
4CIF 704x480	1,0	0,5	0,4	0,7	0,3	0,2
1Mpx 1280x720	2,0	1,1	0,7	1,3	0,7	0,4
2Mpx 1920x1080	4,0	2,7	1,8	2,6	1,8	1,1
3Mpx 2048x1536	6,0	3,4	2,4	3,9	2,2	1,5
4Mpx 2688x1520	8,0	4,5	3,2	5,2	2,6	2,0
5Mpx 2560x1960	9,0	5,5	4,1	5,9	3,1	2,6
8Mpx 3840x2160	16,0	10,0	7,0	10,4	5,9	4,8

zakładamy że klatki kluczowe są wysyłane z częstością 2-3 razy większa niż liczba klatek na sekundę

## 12. Prawidłowe ustawienie modułu kamery kopułkowej

Kamery kopułkowe MAZi IDH-11/21/31/41IR a także pozostałe kamery kopułkowe np. IDH-23/33VR oraz IDH-23/43MR/MRL pozwalają na regulację położenia modułu kamery w pionie oraz w poziomie.

W przypadku maksymalnego pochylenia modułu kamery część diod jest przesłonięta przez obudowę i w nią świeci. W nocy, po włączeniu podświetlenia IR powoduje to odbicie podświetlenia IR od obudowy i powstanie na obrazie silnych odbłasków. Takie ustawienie może być stosowane tylko jeśli wyłączymy podświetlenie w menu kamery: *Menu* → *Konfiguracja Zaawansowana* → *System* → *Obsługa* → *Sprzęt*.

Należy odznaczyć opcję *Włącz podczerwień i zapisać ustawienia – Zapisz*.



*zbyt duże pochylenie – część diod świeci w obudowę*

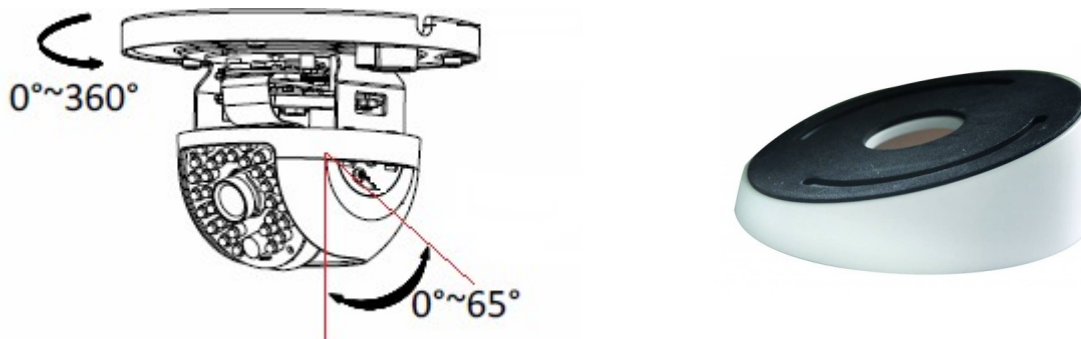


*dopuszczalne pochylenie – wszystkie diody są ponad obudowę*

W celu ustawienia wymaganego pola widzenia kamery przydatna jest ukośna plastikowa podstawa montażowa IJ-D101. Ta podstawa pasuje także do uchwytu IW-D100. W zależności od sytuacji można także zastosować

uchwyt ścienny metalowy IW-D100, plastikowy IW-D101 oraz podstawy montażowe metalowa IJ-D100 a także IJ-V100 czy IW-V100 – zależnie od modelu kamery.

W typowej sytuacji gdy korzystamy z podświetlenia w celu uniknięcia odbicia podświetlenia należy unikać zbyt dużego pochylenia modułu kamery. Diody nie mogą być skierowane na obudowę.



*zakres regulacji modułu kamery IDH-11/21/31/41IR zapewniający brak odbić podświetlenia IR oraz podstawa IJ-D101, kąt pochylenia 15°*

### 13. Zabezpieczenie kamery i połączeń przed wilgocią

- Należy sprawdzić szczelność wszystkich części obudowy kamery np.
  - prawidłowość ułożenia uszczelek między kopułką a obudową, uszczelka musi być równo ułożona, przylegająca do obudowy
  - dokręcenie kopułki do obudowy kamery, należy zwrócić uwagę by pomiędzy obie części nie dostały się przedmioty uniemożliwiające szczelne skręcenie oraz by nie wystawały śruby mocujące obudowę kamery do podłoża lub podstawy, co powoduje nieszczelność pomiędzy kopułką a obudową
  - prawidłowość ułożenia uszczelek między przednią częścią obudowy a tylną częścią obudowy kamery kompaktowej, uszczelka musi być równo ułożona, przylegająca do obudowy
  - dokręcenie przedniej części obudowy do tylnej części obudowy kamery kompaktowej, należy zwrócić uwagę by pomiędzy obie części nie dostały się przedmioty uniemożliwiające szczelne skręcenie
- Kamery MAZi w większości dostarczane są z osłonką zabezpieczającą złącze RJ-45 przed zawilgoceniem.
  - osłonkę należy bezwzględnie stosować, pamiętając o użyciu dołączonej uszczelki
  - niezależnie od jej zastosowania połączenie kablowe musi być zabezpieczone taśmą izolacyjną i taśmą samowulkanizacyjną, zgodnie z ogólnie przyjętymi zasadami zabezpieczania połączeń przed wpływem wody (taśma izolacyjna – taśma samowulkanizująca – taśma izolacyjna)

Niestosowanie się do powyższych wymagań może spowodować zalanie lub zawilgocenie kamery – nie jest to objęte gwarancją.

### 14. Zabezpieczenie kamery przed przepięciami

W przypadku połączeń na zewnątrz, zwłaszcza są to połączenia wychodzące poza obręb jednego budynku należy bezwzględnie stosować zabezpieczenia przeciwprzepięciowe dopasowane do rodzaju połączenia: z lub bez zasilania PoE, połączenia ziemne lub przewieszka.

Uszkodzenia spowodowane przepięciami nie są objęte gwarancją.