Manual de instalare și utilizare Video Interfon analog cu 4 fire Dahua

Ghid de inițiere rapidă

V1.1.0

Cuvânt înainte

General

Acest document introduce în principal structura, instalarea, cablarea și operațiile de meniu ale interfonului video analogic cu 4 fire .

Model

VTH1020J și VTH1020J-T

Instrucțiuni de folosire

Următorul semnal clasificat cu semnificație definită ar putea apărea în manual.

Cuvinte tip semnal	Semnificație
 PERICOL	Indică un pericol potențial ridicat care, dacă nu este evitat, va duce la moarte sau răniri grave.
 ATENȚIE	Indică un pericol potențial mediu sau scăzut care, dacă nu este evitat, ar putea duce la o vătămare ușoară sau moderată.
 PRECAUȚIE	Indică un risc potențial care, dacă nu este evitat, ar putea duce la daune materiale, pierderi de date, performanțe mai mici sau rezultate imprevizibile.
 SFATURI	Oferiți metode care să vă ajute să rezolvați o problemă sau să economisiți timp.
 NOTE	Oferă informații suplimentare ca accent și completare a textului.

Revizuirea istoricului

Versiune	Conținutul revizuirii	Timp de lansare
V1.1.0	• Adăugare de descriere a funcțiilor VTH1020J-T. • S-a adăugat funcția Factory Reset/ Resetare din fabrică	Martie 2021
V1.0.0	Prima apariție	August 2020

Despre Manual

- Nu suntem răspunzători pentru orice pierdere cauzată de operațiunile care nu sunt conforme cu manualul.
- Manualul va fi actualizat în conformitate cu cele mai recente legi și reglementări ale
- jurisdicțiilor conexe.
- Pentru informații detaliate, consultați manualul pe hârtie, CD-ROM, cod QR

  sau site-ul nostru oficial. Dacă există neconcordanță între manualul pe hârtie și versiunea electronică, va prevala versiunea electronică

- Toate proiectele și software-ul pot fi modificate fără o notificare prealabilă scrisă. Actualizările produsului pot cauza unele diferențe între produsul actual și manual. Vă rugăm să contactați serviciul clienți pentru cel mai recent program și documentație suplimentară.

- S-ar putea să existe încă abateri în datele tehnice, descrierea funcțiilor și operațiunilor sau erori de tipărire. Dacăexistă vreo îndoială sau dispută, ne rezervăm dreptul de explicație finală. Dacă manualul (în format PDF) nu poate fi deschis.
- Toate mărcile comerciale, mărcile înregistrate și numele companiilor din manual sunt proprietățile proprietarilor respectivi.
- Vă rugăm să vizitați site-ul nostru web, să contactați furnizorul sau serviciul clienți dacă există probleme la utilizarea dispozitivului.

- Dacă există vreo incertitudine sau controversă, ne rezervăm dreptul la explicații finale.

Măsuri de siguranță și avertismente importante

Următoarea descriere este metoda corectă de aplicare a dispozitivului. Vă rugăm să citiți cu atenție manualul înainte de utilizare, pentru a preveni pericolul și pierderea bunurilor.
Respectați strict manualul în timpul aplicării și păstrați-l corect după citire.

Cerințe de funcționare

- Nu expuneți dispozitivul la lumina directă a soarelui sau la sursa de căldură.
- Nu instalați dispozitivul într-o zonă umedă și murdară.
- Instalați dispozitivul orizontal în locuri stabile pentru a preveni căderea acestuia.
- Nu picurați sau stropiți lichide pe dispozitiv; nu puneți pe dispozitiv nimic umplut cu lichide.
- Instalați dispozitivul în locuri bine ventilate și nu blocați deschiderea de ventilație a acestuia.

Utilizați dispozitivul numai în intervalul nominal de intrare și ieșire.

- Nu demontați singur dispozitivul.
- Dispozitivul trebuie utilizat cu cabluri de rețea ecranate.

Cerinte de putere

- Utilizați cabluri de alimentare recomandate în regiunea sub specificațiile lor.Utilizați o
- sursă de alimentare care îndeplinește cerințele SELV (siguranță la tensiune foarte scăzută) și o sursă de alimentare cu tensiune nominală care este conformă cu sursa de alimentare limitată din IEC60950-1.
  Pentru cerințe specifice de alimentare, vă rugăm să consultați etichetele
- dispozitivului.Cuplajul aparatului este un dispozitiv de deconectare.
  În timpul utilizării normale, vă rugăm să păstrați un unghi care facilitează funcționarea.

Actualizare dispozitiv

Nu întrerupeți alimentarea în timpul actualizării dispozitivului. Sursa de alimentare poate fi întreruptă numai după ce dispozitivul a finalizat actualizarea și a repornit.

Cuprins

Cuvânt înainte ..... **I**
Măsuri de siguranță și avertismente importante ..... **III**
1 Structură **1**
1.1 Introducere 1
1.2 Caracteristici 1
1.3 Panoul frontal 1
1.4 Panou din spate 3
2 Instalare **4**
2.1 VTH 4
2.2 VTO 4
3 Cablare **6**
3.1 Pregătiri 6
3.1.1 Reguli de conectare la port 6
3.1.2 Specificația cablului 7
3.2 Cablarea 1 VTO și 1 VTH 7
3.3 Cablarea 3 VTOs și 1 VTH 8
3.4 Cablare 2 VTOs și 3 VTHs 9
4 Operații Menu **10**
4.1 Instantanee 10
4.2 Timp 1 2
4.3 Restabilirea la setările implicite 12
Appendix 1 Recomandări privind securitatea cibernetică **14**

1 Structură

1.1 Introducere

Interfonul video analogic cu 4 fire constă dintr-o stație de ușă ("VTO") și un monitor de interior ("VTH"). VTH este instalat în interior.

1.2 Caracteristici

VTH

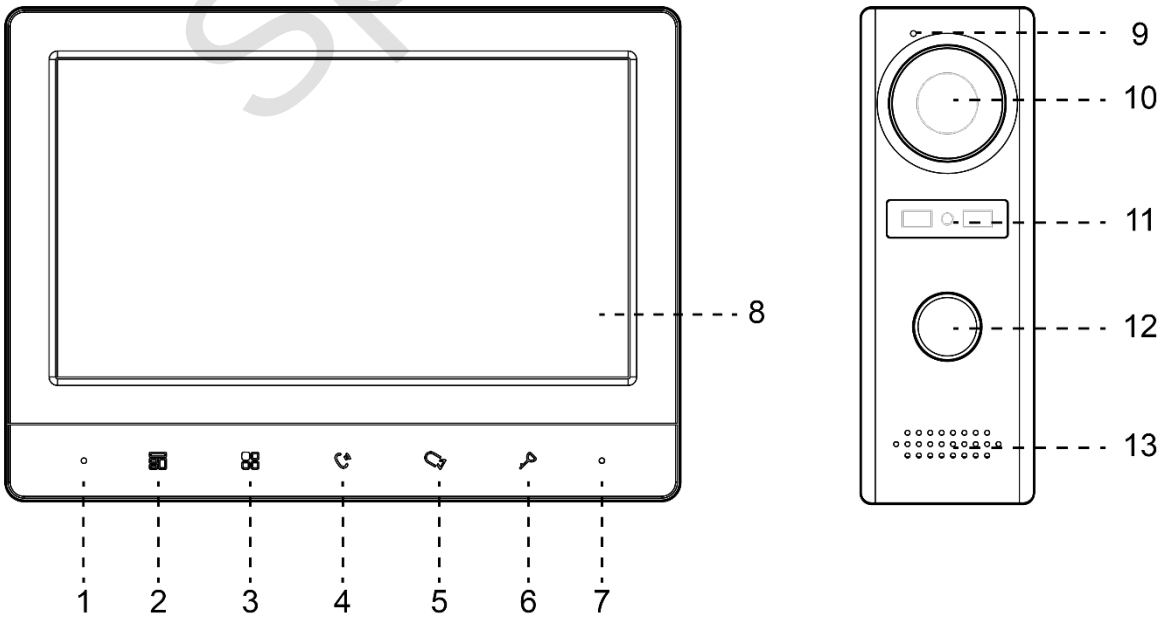
- Comunicare video / voce în timp real
- Poate fi conectat la trei VTO-uri
- Poate fi conectat la camere (CVBS)
- Conectează și utilizează

VTO

- comunicare vocală în timp real
- Iluminare IR autoadaptativă

1.3 Panoul frontal

Figure 1-1 Panou frontal

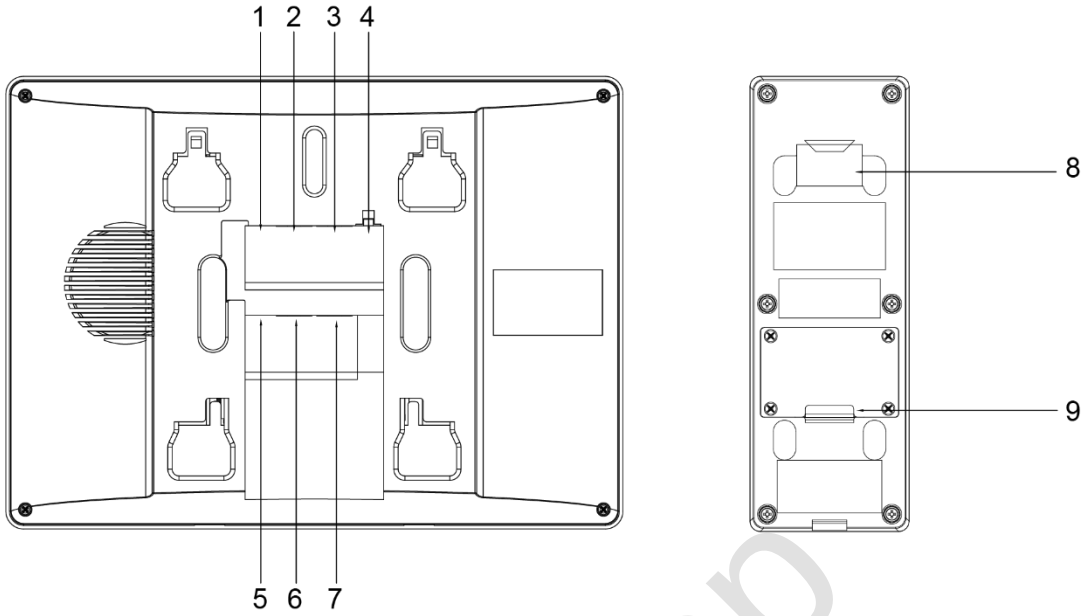


Tabel 1-1 Panou frontal

No.	Pictrograr	Descriere
1	–	Microfon
2		• Apăsați pentru a închide apelul primit. • Faceți instantanee în timpul monitorizării (doar suportat de VTH1020J-T).
3		Trezește ecranul și deschide meniul. Pentru a vedea cum operezi Meniul, uită-te peste "4 Meniul Operațiuni".
4		Când cineva sună de la VTO: • Apăsați o dată pentru a face comunicare vocală cu persoana respectivă. • Apăsați rapid de două ori pentru a închide.
5		Când cineva sună de la VTO: • Apăsați Pentru a vorbi cu persoana (doar suportat de VTH1020J). • Apăsați pentru a face instantanee (doar suportat de VTH1020J-T). Când nu sună nimeni: • Apăsați o dată, de două ori, de trei ori și de patru ori pentru a vizualiza videoclipurile live ale: VTO1, VTO2, camera analogică 1 și respectiv camera analogică 2. • La orice videoclip live, apăsați pentru a face instantanee (suportat de VTH1020J-T).
6		Când cineva sună, apăsați pentru a deschide ușa unde este instalat VTO.
7	–	Indicator de putere.
8	–	ecran LCD .
9	–	Microfon.
10	–	cameră încorporată.
11	–	Indicator de putere.
12	–	Butonul de apelare. • Apăsați o dată pentru a apela VTH • Țineți apăsat timp de 10 secunde pentru a schimba tipul de clopot al TO. Indicatorul de alimentare va clipi. • Apăsați și țineți apăsat timp de 15 secunde pentru a crește volumul soneriei VTO. Indicatorul de alimentare va clipi. Când volumul atinge maxim, acest pas îl va seta la minim. Repetați acest pas pentru a seta volumul adecvat. • Apăsați și țineți apăsat timp de 20 de secunde pentru a trece la modul DWDR (digital wide range dynamic) / modul normal pentru VTO. Indicatorul de alimentare va clipi.
13	–	Difuzor.

1.4 Panoul din spate

Figure 1-2 Panou din spate



Tabel 1-2 Panou din spate

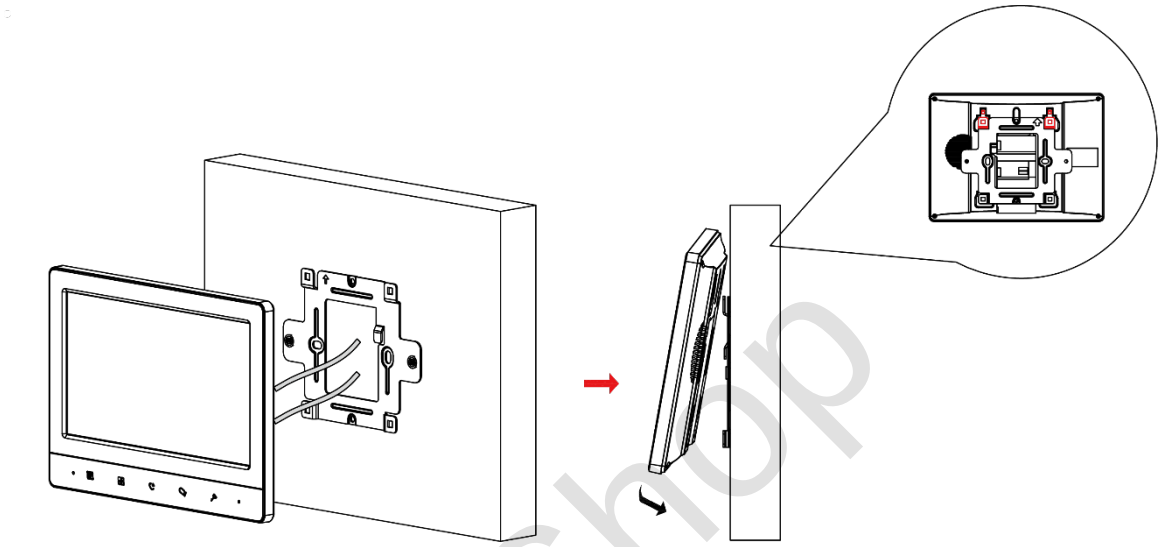
No.	Descriere	No.	Descriere
1	Portul 1 al camerei analogice	6	Portul în cascadă VTH 1.
2	VTO port 1.	7	VTH în cascadă port2.
3	VTO port 2.	8	VTO slot de suspendare.
4	Putere.	9	Fire
5	Portul 2 al camerei analogice.	–	–

2 Instalare

2.1 VTH

Fixați suportul pe perete cu șuruburi, agățați VTH pe suport și apoi aplicați material de etanșare din silicon pe spațiul dintre dispozitiv și perete.

Figure 2-1 Instalare VTH



2.2 VTO

Instalați suportul VTO pe perete, apoi agățați VTO de suport; sau instalați capacul VTO pe perete și apoi atârnați VTO pe capac. În cele din urmă, aplicați etanșant siliconic pe spațiul dintre dispozitiv și perete.

Figure 2-2 Instalare VTO

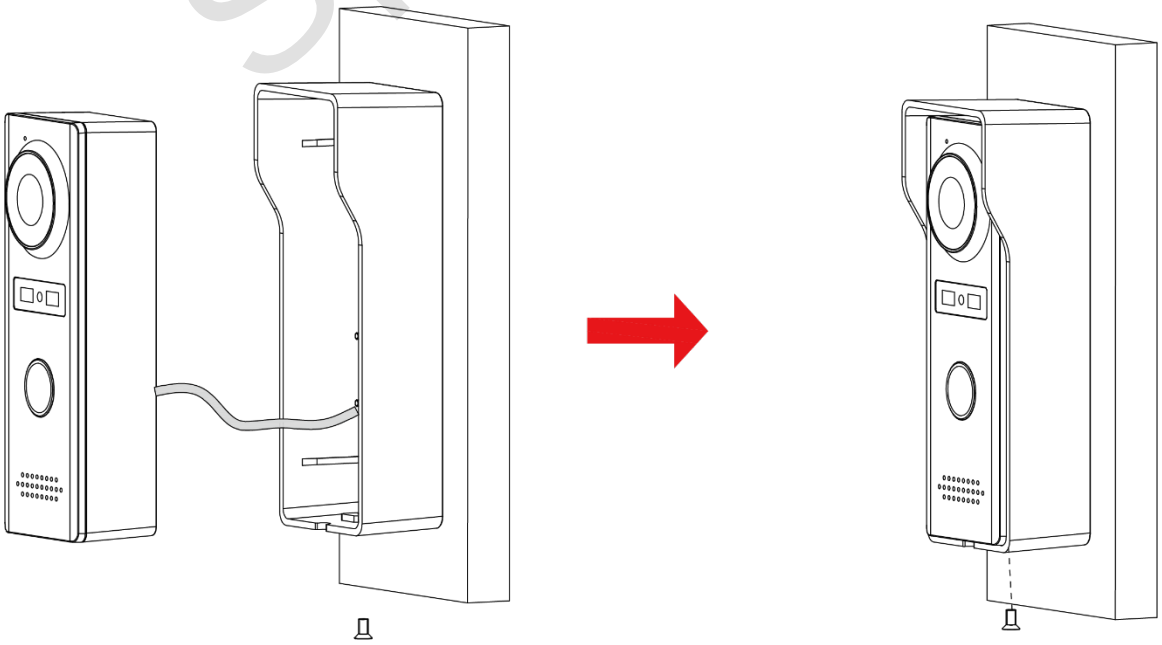
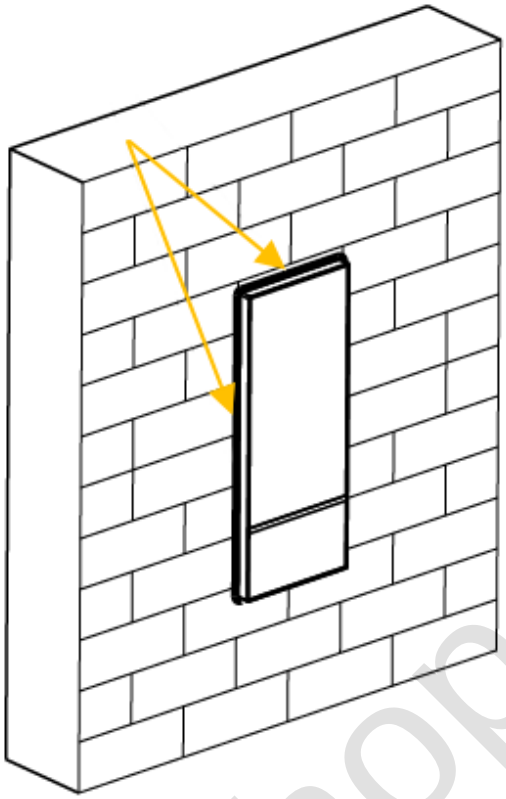


Figure 2-3 Aplicați un material de etanșare siliconic pe spațiul dintre dispozitiv și peretel



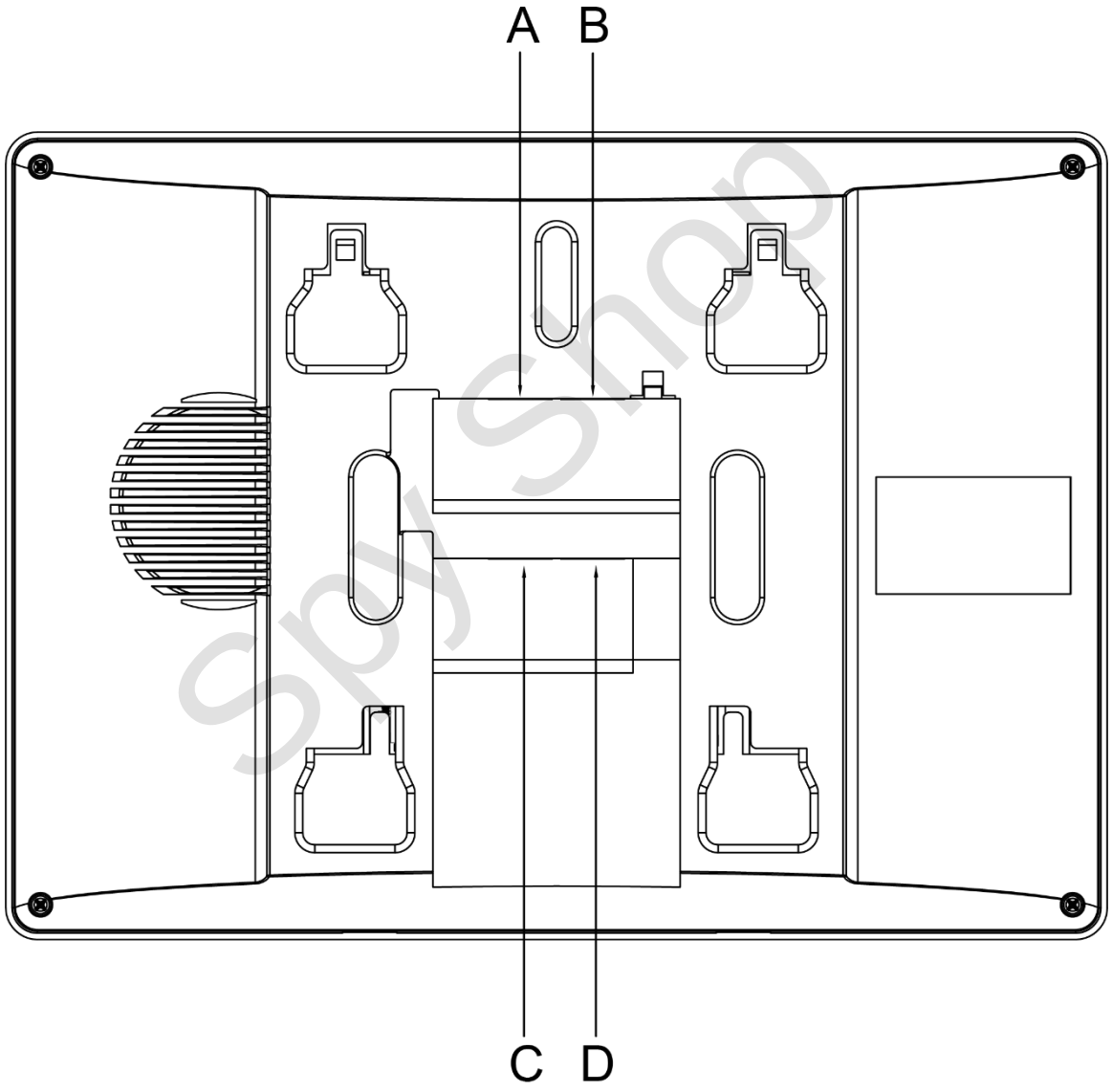
3 Cablare

Cel mult 2 scanări VTO și 3VTH pot fi conectate într-un singur sistem de comunicații.

3.1 Pregătiri

3.1.1 Reguli de conectare la port

Figure 3-1 Reguli de conectare la port



- Portul A al unui VTH poate fi conectat la Portul C al unui alt VTH pentru a face comunicarea de date.
- Portul B al unui VTH poate fi conectat la Portul D al unui alt VTH pentru a face comunicarea de date
- Portul A al unui VTH nu poate fi conectat la Portul B sau D al altui VTH pentru a face comunicarea de date
- Portul C al unui VTH nu poate fi conectat la Portul B sau D al altui VTH pentru a face comunicarea de date .

3.1.2 Specificația cablului

În funcție de distanța dintre VTO și VTH, trebuie să selectați cabluri RVV 4 cu specificații diferite.

Table 3-1 Specificația cablului

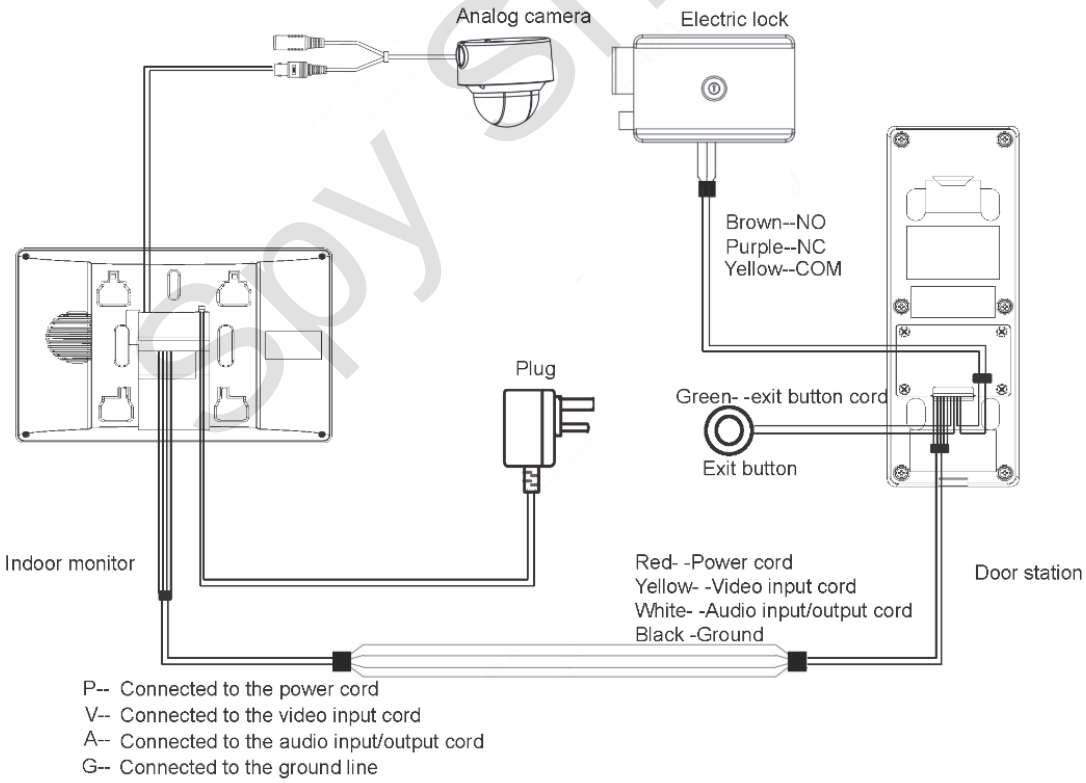
Transmiterea la distanță (TD)	RVV4 Specificația cablului
TD ≤ 10 m	RVV4 × 0.3 mm²
10 m < TD ≤ 30 m	RVV4 × 0.5 mm²
30 m < TD ≤ 50 m	RVV4 × 0.75 mm²

Dacă distanța dintre VTO și VTH estemai mult de 50m, utilizați cabluri coaxiale.

- Nu trageți cordoanele violent.
- În timpul cablării, înfășurați îmbinările cablului cu bandă de cauciuc izolată pentru a preveni scurtcircuitul.

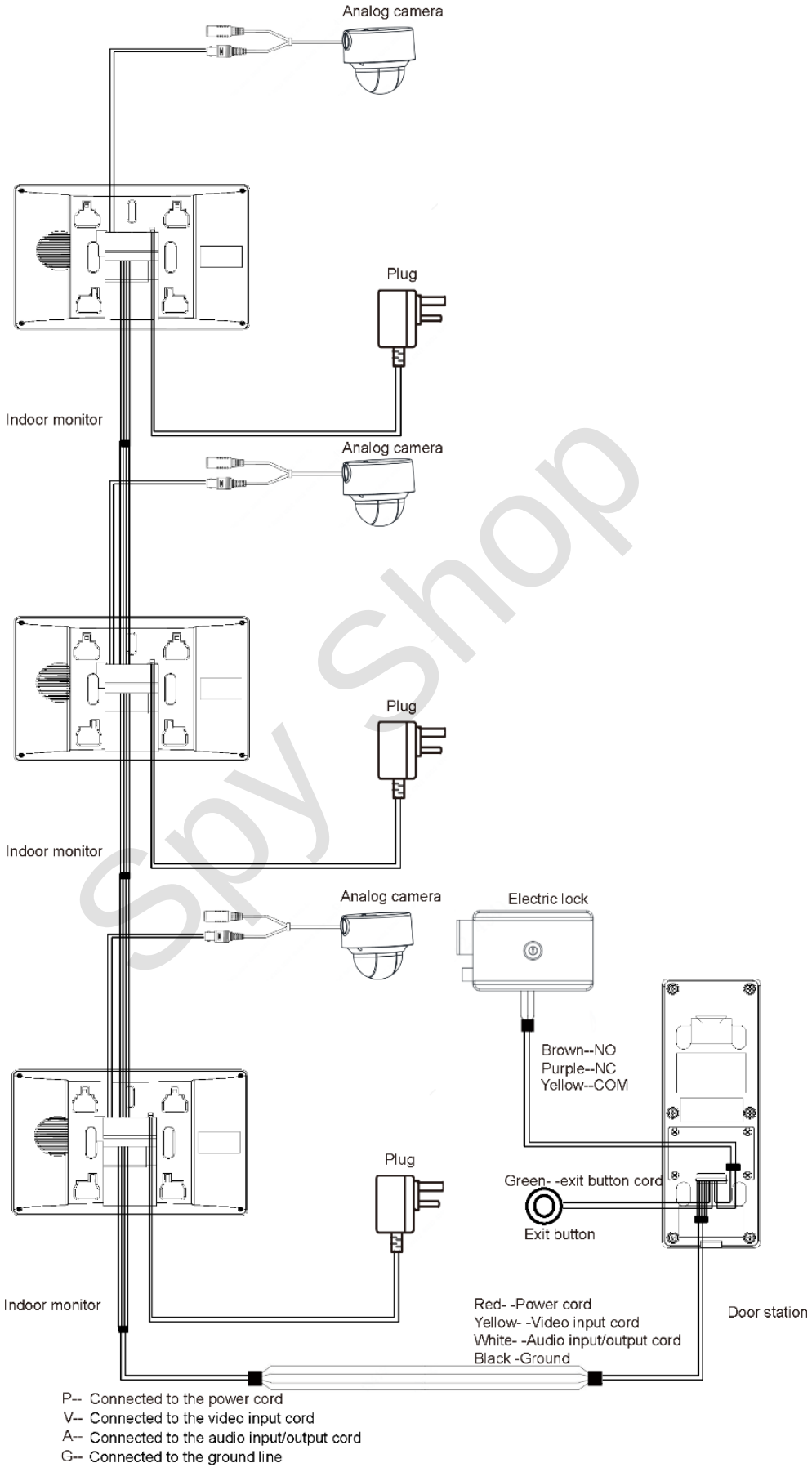
3.2 Cablare Un VTO și Un VTH

Figure 3-2 Cablare(1)



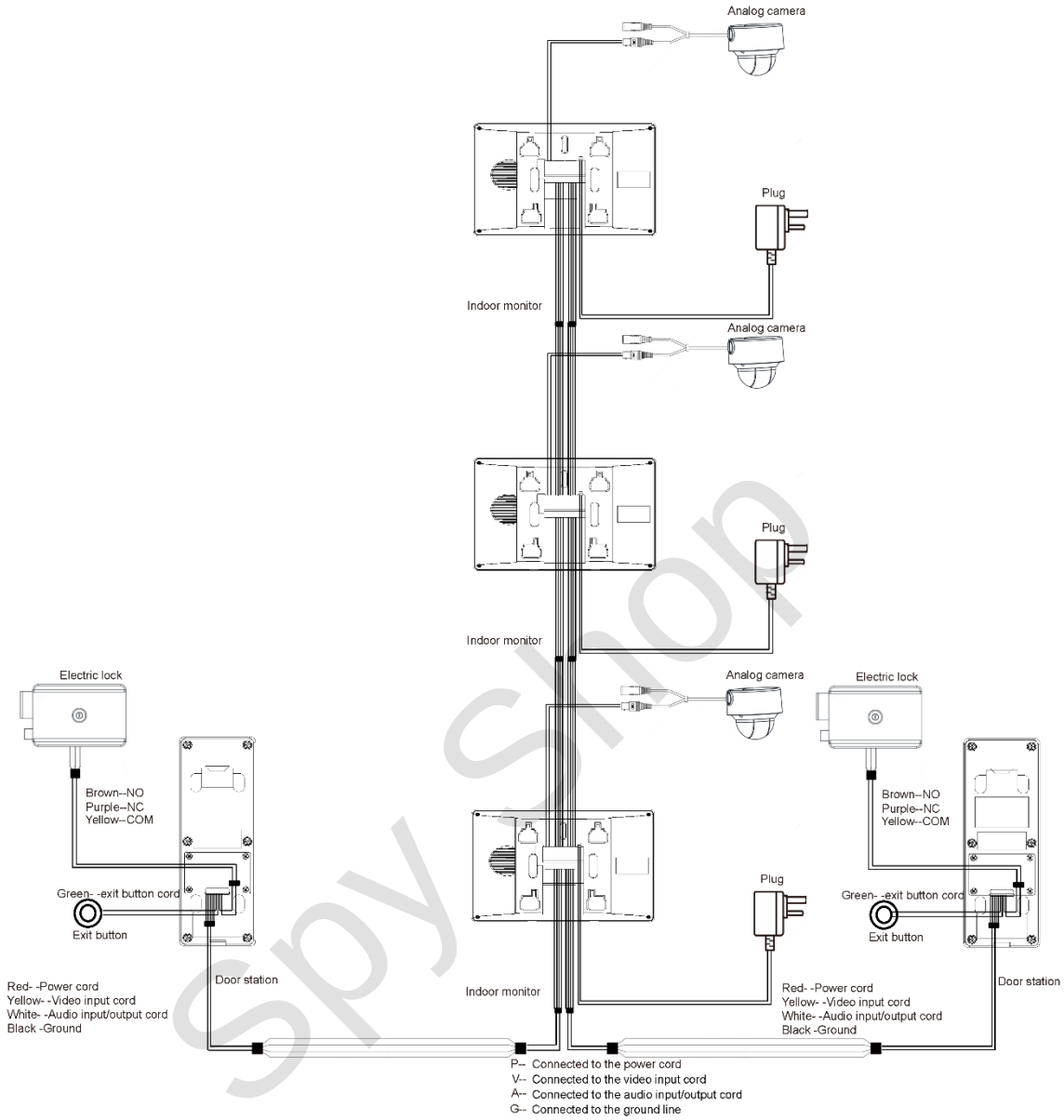
3.3 Cablarea a trei VTO-uri și a unui VTH

Figure 3-3 Cabalare(2)



3.4 Cablarea a două VTO-uri și trei VTH-uri

Figure 3-4 Cablare(3)



Camerele analogice recomandate (CVBS) sunt seria HAC 1230.

4 Meniul Operațiuni

Puteți configura funcțiile VTH, cum ar fi volumul, luminozitatea și multe altele.

- Numai VTH1020J-T acceptă Instantanee și Funcții de timp.
- Toate configurațiile vor fi salvate după ce ieșiți din meniu.

Figure 4-1 Meniu

Table 4-1 Operații meniu

Pictograme	Funcții
	Folosit pentru a vă confirma funcționarea atunci când utilizați funcțiile Instantanee și timp (acceptate numai de VTH1020J-T).
	Reglați Vol (volum), Luminozitate (luminozitate), Contrast și Vol Bell (volum sonerie), schimbați Bell și opriți DND (nu deranjați).
	Creșteți Vol (volum), Luminozitate (luminozitate), Contrast și Vol Bell (volum sonerie), schimbați Bell, opriți DND (nu deranjați) și reglați ora.
	Selectează un item .
	• Ieșiți din meniu și blocați ecranul. • Reveniți la interfața anterioară.

4.1 Instantanee

Puteți face instantanee în timpul monitorizării și puteți vizualiza instantaneele pe care le-ați făcut.

VTH poate stoca până la 200 de instantanee. Dacă stocarea este plină, cele anterioare vor fi suprascrise.

Realizarea instantaneelor

- În timpul monitorizării

Step 1 Apasă pentru a accesa imaginea de monitorizare dorită.

Step 2 Apasă , iar apoi Successful va apărea pe ecran.

- Când un VTO sună sau într-un apel cu un VTO, apăsați ,și apoi Successful va apărea pe ecran.

Dacă apelul durează mai mult de 1 secundă, instantaneul va fi realizat automat.

Vizualizarea instantaneelor

Step 1 Apasă pentru a afișa meniul.

Step 2 Apasă , selectați Instantanee, apoi apăsați .

Figure 4-2 Lista instantaneelor

Step 3 Apasă pentru a selecta cea de care aveți nevoie, apoi apăsați .

Pentru a șterge instantaneul, , Șterge? o să apară pe ecran, apoi apasă și apăsă confirmă.

Figure 4-3 Vizualizarea unui instantaneu

Step 4 Apasă sau pentru a vizualiza instantaneul anterior sau următor. Sau puteți apăsa pentru a vă întoarce la lista instantaneelor, apoi selectați-l pe cel de care aveți nevoie.

Pentru a șterge un instantaneu, apasă , Șterge? o să apară pe ecran, și apoi apasă pe confirmă

4.2 Timp

Step 1 Apasă pentru a afișa meniul.

Step 2 Apasă pentru a selecta partea de timp dorită.

Step 3 Apasă pe sau pentru a ajusta numărul.

4.3 Restabilirea la setările implicite

Step 1 Apasă pentru a afișa meniul.

Step 2 Apasă pentru a selecta Resetare din fabrică.

Figure 4-4 Confirmați-vă operațiunea

Step 3 Apasă , și apoi dispozitivul va reporni.

Appendix 1 Recomandări privind securitatea cibernetică

Securitatea cibernetică este mai mult decât un simplu cuvânt la modă: este ceva ce ține de fiecare dispozitiv conectat la internet. Supravegherea video IP nu este imună la riscurile cibernetice, dar luarea măsurilor de bază către protejarea și consolidarea rețelelor și a dispozitivelor din rețea le va face mai puțin susceptibile la atacuri. Mai jos sunt câteva sfaturi și recomandări despre cum să creați un sistem de securitate mai securizat.

Acţiuni obligatorii care trebuie întreprinse pentru securitatea de bază a reţelei dispozitivului:

1. Folosește parole puternice

Vă rugăm să consultați următoarele sugestii pentru a seta parolele:

- Lungimea nu trebuie să fie mai mică de 8 caractere;
- Includeți cel puțin două tipuri de caractere; tipurile de caractere includ majuscule și minuscule, cifre și simboluri;
- Nu conține numele contului sau numele contului în ordine inversă;
- Nu utilizați caractere continue, cum ar fi 123, abc, etc .;
- Nu utilizați caractere suprapuse, cum ar fi 111, aaa etc .;

2. Actualizați firmware-ul și software-ul clientului la timp

- Conform procedurii standard din industria tehnologică, vă recomandăm să vă actualizați firmware-ul dispozitivului (cum ar fi NVR, DVR, cameră IP etc.) pentru a vă asigura că sistemul este echipat cu cele mai recente patch-uri și remedieri de securitate. Când dispozitivul este conectat pentru rețeaua publică, se recomandă să activați funcția „verificare automată pentru actualizări" pentru a obține informații în timp util despre actualizările de firmware lansate de producător.
- Vă sugerăm să descărcați și să utilizați cea mai recentă versiune a software-ului client.

Recomandări „Îmi face plăcere" pentru a îmbunătăți securitatea rețelei dispozitivului:

1. Protecție fizică

Vă sugerăm să efectuați protecție fizică a dispozitivului, în special a dispozitivelor de stocare. De exemplu, așezați dispozitivul într-o sală specială de calculatoare și dulapuri și implementați permisiunea de control al accesului și gestionarea cheilor bine făcute pentru a preveni personalul neautorizat care efectuează contacte fizice precum hardware, conexiunea neautorizată a dispozitivului amovibil (cum ar fi discul USB flash, seria port) etc.

2. Schimbă parola regulat

Vă sugerăm să modificați parolele în mod regulat pentru a reduce riscul de a fi ghicit sau spart.

3. Setați și actualizați parolele Resetați informațiile în timp util

Dispozitivul acceptă funcția de resetare a parolei. Configurați informațiile aferente pentru resetarea parolei la timp, inclusiv căsuța poștală a utilizatorului final și întrebările privind protecția parolei. Dacă informațiile se modifică, vă rugăm să le modificați la timp. Când setați întrebări de protecție prin parolă, nu este sugerat să folosiți cele care pot fi ușor ghicite.

4. Activați blocarea contului

Funcția de blocare a contului este activată în mod implicit și vă recomandăm să o continuați garantează securitatea contului. Dacă un atacator încearcă să se conecteze cu o parolă greșită de mai multe ori, contul corespunzător și adresa IP sursă vor fi blocate.

5. Schimbați HTTP și alte porturi de servicii implicite

Vă sugerăm să modificați porturile HTTP și alte porturi de servicii implicite în orice set de numere între 1024 ~ 65535, reducând riscul ca persoanele din afară să poată ghici ce porturi utilizați.

6. Activați HTTPS

Vă sugerăm să activați HTTPS, astfel încât să vizitați serviciul Web printr-un canal de comunicare securizat.

7. Legare adresă MAC

Vă recomandăm să legați adresa IP și MAC a gateway-ului de dispozitiv, reducând astfel riscul de falsificare ARP.

8. Atribuiți conturi și privilegii în mod rezonabil

În conformitate cu cerințele de afaceri și de gestionare, adăugați în mod rezonabil utilizatori și atribuiți-le un set minim de permisiuni.

9. Dezactivați serviciile inutile și alegeți moduri sigure

Dacă nu este necesar, se recomandă oprirea unor servicii precum SNMP, SMTP, UPnP etc., pentru a reduce riscurile.Dacă este necesar, este foarte recomandat să utilizați moduri sigure, inclusiv, dar fără a se limita la următoarele servicii:

- SNMP: Alege SNMP v3, și configurați parole puternice de criptare și parole de autentificare.
- SMTP: Alegeți TLS pentru a accesa serverul de cutii poștale.
- FTP: Alegeți SFTP și configurați parole puternice.
- Hotspot AP : Alegeți modul de criptare WPA2-PSK și configurați parole puternice.

10. Transmisie criptată audio și video

În cazul în care conținutul dvs. de date audio și video este foarte important sau sensibil, vă recomandăm să utilizați funcția de transmisie criptată, pentru a reduce riscul ca datele audio și video să fie transmise permanent.

Memento: transmisia criptată va provoca unele pierderi în eficiența transmisiei.

11. Audit securizat

- Verificați utilizatorii online: vă sugerăm să verificați în mod regulat utilizatorii online pentru a vedea dacă dispozitivul este conectat fără autorizare.
- Verificați jurnalul dispozitivului: Vizualizând jurnalele, puteți cunoaște adresele IP care au fost utilizate pentru a vă conecta la dispozitivele dvs. și operațiunile cheie ale acestora.

12. Jurnal de rețea

Datorită capacității limitate de stocare a dispozitivului, jurnalul stocat este limitat. Dacă trebuie să salvați jurnalul pentru o lungă perioadă de timp, se recomandă să activați funcția jurnal de rețea pentru a vă asigura că jurnalele critice sunt sincronizate cu serverul de jurnal de rețea pentru urmărire.

13. Construiți un mediu de rețea sigur

Pentru a asigura mai bine siguranța dispozitivului și a reduce potențialele riscuri cibernetice, vă recomandăm:

- Dezactivați funcția de mapare a porturilor routerului pentru a evita accesul direct la dispozitivele intranet din rețeaua externă.
- Rețeaua trebuie să fie partiționată și izolată în funcție de nevoile actuale ale rețelei. Dacă nu există cerințe de comunicare între două subrețele, se recomandă

  folosirea VLAN, rețea GAP și alte tehnologii pentru partiționarea rețelei, astfel încât să se obțină efectul de izolare a rețelei.
- Stabiliți sistemul de autentificare cu acces 802.1x pentru a reduce riscul accesului neautorizat la rețelele private.
- Activați funcția de filtrare a adreselor IP / MAC pentru a limita gama de gazde permise pentru a accesa dispozitivul