(19) DANMARK

PATENTDIREKTORATET
TAASTRUP

(12) **FREMLÆGGELSESSKRIFT** (11) **157644 B**

(21) Patentansøgning nr.: **4103/82**

(22) Indleveringsdag: **14 sep 1982**

(41) Alm. tilgængelig: **16 mar 1983**

(44) Fremlagt: **29 jan 1990**

(86) International ansøgning nr.: -

(30) Prioritet: **15 sep 1981 DE 3136461**

(51) Int.Cl.[5] **H 04 L 1/16**
H 04 K 1/00

(71) Ansøger: ***SIEMENS AKTIENGESELLSCHAFT; Wittelsbacherplatz 2; 8000 München 2; Berlin und München, DE**

(72) Opfinder: **Manfred *Hanni; DE, Josef *Brusch; DE**

(74) Fuldmægtig: **Internationalt Patent-Bureau**

(54) Fremgangsmåde til sikret overføring af digitale signaler

(56) Fremdragne publikationer

———

(57) Sammendrag:

4103-82

Der tilsigtes ved kommunikationsforbindelser over kortbølger en stor modstandsdygtighed over for bevidst fremmed støj, og hertil angives følgende sammenhængende foranstaltninger.

a) Sende- og modtagestationerne udrustes med meget konstante kvartsure (QH), og til de signalblokke (burster), der skal overføres, tilføjes der et tidssignal, ved hjælp af hvilket mulige tidstolerancer mellem stationerne kan korrigeres.

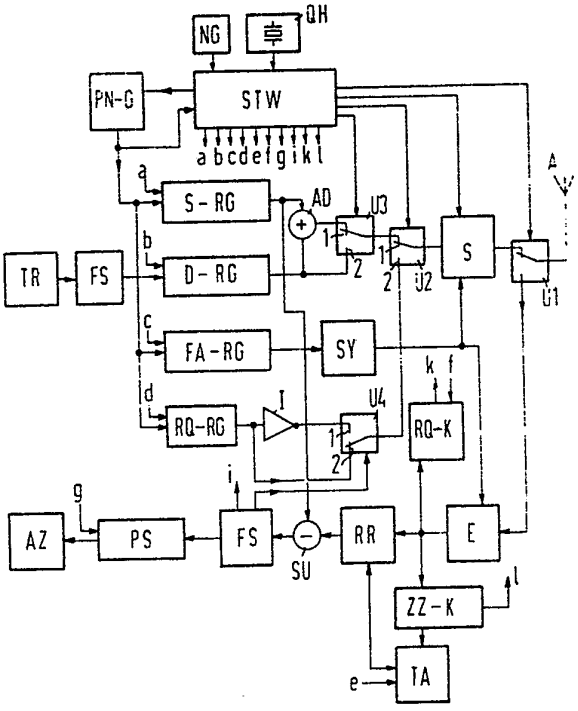
b) Under anvendelse af en ARQ (Automatic request) gøres der brug af en frekvensvariation af radiofrekvensen i rytme med efter hinanden følgende burstsendinger under inkludering af kvitteringsreturmeldingen.

c) Den i bursten fejlsikret indeholdte information overføres chiffreret.

d) Chiffreringsfølgen for chiffreringen af burstens informationsdel og fejlsikringsdel og for den sendefrekvensen henholdsvis modtagefrekvensen bestemmende frekvensadresse bliver på grundlag af kvartsurets (QH) klokketidspunkt og ordenstnummeret nyberegnet for hver burst.

FIG 1

4103-82



DK 157644 B

Opfindelsen angår en fremgangsmåde til sikret overføring af digitale signaler, navnlig data via kortbølge, hvor de med en datasikring forsynede chiffrerede signaler overføres blokvist (burst) fra en sende- til en modtagestation, og hvor der fra modtagestationen før udsendelse af en yderligere burst tilbageoverføres et kvitteringssignal til sendestationen (automatic request).

Fremgangsmåder af denne art er eksempelvis beskrevet i en bog af L. Wiesner "Fernschreib- und Datenübertragung über Kurzwelle", 3. oplag, 1980, siderne 105-114 og 184-188. Den blokvise overføring med kvittering i forbindelse med en datasikring gør det på modtagesiden let muligt at befri forstyrrede burster for overføringsfejl i henseende til deres informationsindhold. Derudover kan den samme blok om nødvendigt udsendes endnu engang, hvis det over tilbagesvaret på sendestationen erkendes, at informationsblokken på modtagesiden er ankommet ukorrigerbart defekt. Endvidere muliggør chiffreringen en aflytningssikker overføring.

Denne metode til sikret overføring er imidlertid ikke tilstrækkelig, hvis der skal regnes med bevidste forstyrrelser. Sådanne bevidste forstyrrelser skal der i hvert fald altid regnes med i radiosystemer til taktisk anvendelse. Ganske vist gør sådanne radioanlæg som regel brug af et i forhold til kortbølgeområdet væsentligt højere frekvensområde, men i praksis er anvendelse af kortbølgeområdet af og til uundgåelig som følge af ugunstige terræn- og/eller afstandsforhold. I disse tilfælde er det derfor nødvendigt at træffe særlige forholdsregler til sikring af informationsoverføringen i dette område.

Til en sikker kortbølgeoverføring med enkle midler er datahastigheden begrænset til ca. 200 bit/s. Som minimal informationsmængde anses 3 byte svarende til 24 bit. Under hensyntagen til den yderligere datasikring fremkommer der her mindste længder for de informationspakkerne udgørende burster > 200 ms. Hvis den, der vil forstyrre, er bekendt med forbindelsens frekvens, er en

sådan burstlængde allerede med henblik på kommende teknologier for høj. Det viser sig også, at den forholdsvis lange indbyrdes indfasningsprocedure mellem to stationer, som træder i forbindelse med hinanden, før den egentlige overføring er ualmindelig støjpåvirkelig. Hvis det ved målrettede foranstaltninger lykkes en forstyrrer at forstyrre forbindelsesopbygningen, bliver en informationsoverføring på denne måde på forhånd umulig.

Opfindelsen tager sigte på at angive en løsning for en digital informationsoverføring, navnlig på kortbølger, som foruden aflytningssikkerhed også udviser en tilstrækkelig høj resistens mod bevidst forstyrrelse.

Med udgangspunkt i en fremgangsmåde til sikret overføring af digitale signaler, navnlig data, over kortbølger løses denne opgave ifølge opfindelsen ved samvirke mellem de i krav 1's kendetegnende del angivne foranstaltninger.

Ved opfindelsen gås der ud fra den erkendelse, at ved anvendelse af meget nøjagtige stationskvartsure kan tiden til forbindelsesopbygningen i sammenhæng med en tidssignaloverføring holdes meget kort. Ydermere forhindres en bevidst forstyrrelse af bursterne effektivt ved en stadig variation af radiofrekvensen fra en burst til den næste. Ved anvendelse af frekvensspring kan de benyttede frekvenser ganske vist ikke reserveres eller undersøges på forhånd med hensyn til støjfrihed. Heller ikke fadingforholdene kan forudsiges. Ved samtidig anvendelse af frekvensspring i forbindelse med automatisk tilbagemelding i form af et kvitteringssignal (ARQ) kan der imidlertid alligevel foretages en sikker dataoverføring, omend den er langsom. Med henblik på at gøre det væsentligt vanskeligere for en aktiv forstyrrer at erkende kvitteringssignalet bliver dette ligeledes kun overført på chiffreret form.

Hvis omfanget af den signalinformation, der skal overføres, er så ringe, at den kan overføres i en enkelt burst, er det lidet hensigtsmæssigt at sætte en kaldeburst foran en sådan enkelt burst. Et specielt opkald er

for så vidt heller ikke nødvendigt, som den i samvirke med det indstillede kaldenummer udkodede chiffreringsfølge har selektive opkaldegenskaber. Opkaldet er på sin vis integreret i bursten over chiffreringen. Fordelagtigt omfatter derfor hver enkeltburst en chiffreret informationsdel, en ligeledes chiffreret fejlsikringsdel og en foran disse to dele stillet uchiffreret tidssignaldel, som ved modtagesidens udnyttelse i en tidssignalkorrelator anvendes til indstilling af den rigtige modtagefase.

Hvis den signalinformation, der skal overføres, skal fordeles på et antal efter hinanden følgende burster, er det hensigtsmæssigt, at der foran den informationsburst, der skal overføres, og som omfatter en chiffreret informationsdel og en chiffreret fejlsikringsdel, sættes en kaldeburst, som omfatter et tidssignal og en chiffreringsfølge, der udgør selektivkaldet, hvilken kaldeburst efter modtagelse og erkendelse af opkaldet på den modtagende station foranlediger udsendelse af kvitteringssignalet med en fast forudbestemt tidsafstand, som står i relation til det modtagne tidssignal. Ud fra modtagetiden for dette kaldebursten kvitterende kvitteringssignal på den kaldende station indstilles et snævert tidsvindue til modtagelse af yderligere kvitteringssignaler i forbindelse med den efterfølgende overføring af informationsburster. På denne måde opnås det på overordentlig fordelagtig måde, at sandsynligheden for, at kvitteringssignalet trods chiffreringen erkendes, er tilstrækkelig stor. Tidsvinduet nedsætter nemlig i væsentlig grad sandsynligheden for en efterligning af kvitteringssignalet som følge af støj.

Mens det ved overføringen af enkeltburster gælder, at det enkeltbursten tilføjede tidssignal muliggør en burstindividuel korrektion af modtagesidens taktfase, foreligger denne mulighed ikke ved den forannævnte overføring af en signalinformation, som omfatter et stort antal informationsburster. Den synkronisering, som tilvejebringes af det i kaldebursten overførte tidssignal,

kan ikke forhindre, at der som følge af løbetidsvariationer under overføringen af de efter kaldebursten følgende informationsburster kan optræde fasevariationer som følge af løbetidsændringer. Sådanne løbetidsvariationer kan imidlertid indtil en ændring i størrelsesordenen en halv bit på fordelagtig måde beherskes ved, at hver ankommende bit i en informationsburst på modtagesiden før dechiffreringen indlæses i flere faser, f.eks. otte faser, i en matrikslager. Over en bestemmelse af de bitfasespalter, der udmærker sig ved et mindsteantal af bitspringovergange, foretages der en fastlæggelse af modtagesidens taktfase for hver ankommende informationsburst for midten af dette bitfasespalteområde, og derpå bliver den til denne taktfase knyttede bitfasespalte dechiffreret og tilført fejlsikringen.

Ved hjælp af et sådant matrikslager kan også løbetidsvariationer, som overstiger en halv bit, beherskes ved, at de i flere faser indlæste ankommende bit i en informationsburst dechiffreres ordnet efter deres bitfasespalter og tilføres fejlsikringen. Til fastlæggelse af modtagesidens taktfase bestemmes da en af modtageren til informationsafgivelse sluttelig også antaget bitfasespalte, som er fejlfri henholdsvis fejlkorrigerbar.

Med henblik på også at forhindre, at en forstyrrer i rytme med de på hinanden følgende burster kan imitiere tidssignaler eller anden signalinformation, hvilket ville svare til en uønsket forøgelse af fejlalarmeringshyppigheden, foreslås det ifølge en videreudvikling af opfindelsen, at tidsintervallet mellem to på hinanden følgende sendetidspunkter for udsendelse af en burst ændres pseudotilfældigt inden for forudbestemte grænser ved hjælp af chiffreringsudstyret.

Opfindelsen er i det følgende forklaret nærmere på grundlag af nogle udførelseseksempler, som er vist på tegningen, hvor

fig. 1 viser et blokdiagram over en første sende-modtagestation, som arbejder efter fremgangsmåden ifølge

opfindelsen,

fig. 2 et tidsdiagram, som nærmere forklarer funktionen af den i fig. 1 viste sende-modtagestation,

fig. 3 et blokdiagram over en anden sende-modtagestation, som arbejder efter fremgangsmåden ifølge opfindelsen,

fig. 4 et tidsdiagram, som forklarer forløbet af en forbindelsesopbygning mellem to stationer som vist i fig. 3,

fig. 5 et yderligere tidsdiagram, som forklarer driftsforløbet for to stationer som vist i fig. 3, og

fig. 6 en tabel, som nærmere forklarer virkemåden af matrikslageret i den i fig. 3 viste station.

Den i fig. 1 viste sende-modtagestation til enkeltsignaldrift har en sende-modtageantenne A, som over en sende-modtageomskifter U1 valgfrit er koblelig med den egentlige sender S henholdsvis med den egentlige modtager E. Sende-modtagestationen har eksempelvis en ved hjælp af en mikroprocessor realiseret styreenhed STW, som også samarbejder med det meget nøjagtige digitale kvartsur QH og med kaldenummergiveren NG. Styreenheden STW har en række taktudgange a, b, c, d, e, f og g samt styreinformationsindgange i, k og l, hvis forbindelser til de øvrige blokke, der skal beskrives i det følgende, blot er antydet ved korte pile og angivelse af de nævnte bogstavbetegnelser. Styreenheden STW samarbejder endvidere med en en chiffreringsfølge leverende pseudotilfældighedsgenerator PN-G, som dels på udgangssiden stiller en impulsfølge til rådighed for styreenheden STW, dels af styreenheden over en yderligere forbindelsesledning før begyndelsen af en burstoverføring indstilles i en af klokketidspunktet og kaldenummergiveren NG's indstilling afhængig starttilstand. Med andre ord bliver der i hvert enkelt tilfælde før begyndelsen af et sendevindue for en burst på denne måde på grundlag af klokketidspunktet og det i kaldenummergiveren NG indstillede abonnentnummer beregnet en chiffreringsfølge. Som følge af den i form af den

chiffrerede information overførte chiffreringsfølges opkaldselektive egenskaber kan denne kun dechiffreres på den opkaldte station, hvorved det sikres, at kun den, der til den samme tid har indstillet den samme døgnkode og det samme kaldenummer, kan opfatte opkaldet.

Under antagelse af, at hver i fig. 2 viste burst Be i henseende til sin informations- og fejlsikringsdel IN og ECD skal chiffrere 36 bit, bliver der fra udgangen på pseudotilfældighedsgeneratoren PN-G ladet 36 bit i chiffreringsregistret S-RG, 7 bit i kvitteringssignalregistret RQ-RG og 16-30 bit (alt efter anvendelsen) i frekvensadresseregistret FA-RG. Den i frekvensadresseregistret FA-RG ladede chiffreringsdelfølge bestemmer over adresseindgangen på syntesizeren SY sendefrekvensen i senderen S og modtagefrekvensen i modtageren E, som herved i hvert enkelt tilfælde er lig med hinanden. Den information, der skal overføres, bliver over tastaturet TR og fejlsikringen FS indgivet i dataregistret D-RG.

Ved begyndelsen af det til udsendelse af en burst Be forudgivne tidsvindue bliver først det i dataregistret D-RG's begyndelsesdel fast forbundne tidssignal ZC (fig. 2) i form af en barkerkode over en omskifter U3 og en omskifter U2 tilført senderen S. Dertil leverer styreenheden STW de nødvendige takter, og den stiller omskifteren U3 i koblestilling 2. Derefter bliver omskifteren U3 igen stillet tilbage til den i fig. 1 viste koblestilling 1, og yderligere forsynes chiffreringsregistret S-RG med styretakter. Derved bliver den egentlige information med den efterfølgende fejlsikringsdel chiffreret i chiffreringsapparatet AD og ligeledes tilført senderen S over de to omskiftere U3 og U2.

Den sendende og den fjerne modtagende station er i langtidssynkronisme med hinanden, hvilken synkronisme opretholdes ved hjælp af de meget præcise stationskvartsure QH. Mulige fasefejl korrigeres på modtagesiden ved tidssignalernes ankomst.

Ved en ankommende burst over sende-modtageantennen A er sende-modtageomskifteren U1 i den stilling, som er antydet ved hjælp af en med punkterede linier indtegnet koblearm, og i hvilken signalet bliver tilført modtageren E. Modtageren tilfører over sin udgang det burstbegyndelsen udgørende tidssignal til tidssignal-korrelatoren ZZ-K, som under varigheden af det på modtagesiden hertil forhåndenværende, i fig. 2 med ZF-KS betegnede tidsvindue iagttager tidssignal-korrelationsspidsens opståen og ved sin konstatering over taktudnyttelsen TA foranlediger, at de efterfølgende 36 bit med den ved korrelationen bestemte taktfase regenereres i den efter modtageren E indkoblede regenerator RR og derpå dechiffreres i dechiffreringsapparatet SU. Hertil får dechiffreringsapparatet over den anden indgang igen tilført det i chiffreringsskifteregistret S-RG lagrede chiffreringssignal. Den efter dechiffreringsapparatet SU indkoblede fejlsikring FS tilfører informationen, såfremt den har konstateret dennes fejlfrihed henholdsvis kan korrigere en forhåndenværende fejl, til pufferlageret PS, over hvilket informationen derefter fremstilles på en indikeringsindretning AZ.

Straks efter bearbejdningen af den sidste informationsbit skifter den bursten modtagende sende-modtagestation over sende-modtageomskifteren U1 fra modtagelse til udsendelse og kvitterer for den korrekt modtagne burst ved afgivelse af det i kvitteringssignalregistret RQ-RG lagrede kvitteringssignal over omskifteren U4 og omskifteren U2, som hver især er i koblestilling 2, til senderen S, som over sende-modtageomskifteren U1 og sende-modtageantennen A udsender kvitteringssignalet til den fjerne station. Hvis der ikke registreres nogen korrekt modtaget burst, sker udsendelsen af kvitteringssignalet på inverteret form. Hertil styrer fejlsikringen FS på modtagesiden omskifteren U4 i koblestillingen 1, således at det fra kvitteringssignalregistret RQ-RG afgivne kvitteringssignal når frem

til senderen over inverteren I.

Den sende-modtagestation, der har udsendt bursten, kobler sin sende-modtageomskifter U1 i den med punkterede linier tegnede koblestilling og dermed til modtagelse, såsnart bursten er udsendt. Det ankommende kvitteringssignal bliver over modtageren E tilført modtagesidens kvitteringssignalkorrelator RQ-K, som videresignalerer korrelationsresultatet til styreenheden STW. Uafhængigt af korrelationsresultatet forbereder styreenheden STW udsendelsen af en yderligere burst. Ved et positivt korrelationsresultat bliver hertil først dataregistret D-RG ladet med en ny information, mens dette imidlertid udebliver ved et negativt resultat. På denne måde sørges der for, at den yderligere burst, der skal udsendes, med hensyn til sit nyttesignalindhold ved et negativt resultat stemmer overens med den forudgående burst. Ændringen af sendefrekvensen og af chiffreringssignalet, som udkodes på-ny for hver burst på grundlag af klokketidspunktet, samt sendetiden, der ændres pseudotilfældigt inden for forudgivne grænser, berøres ikke af kvitteringssignalkorrelatorens korrelationsresultat.

Ved hjælp af de kun til bestemte tidspunkter til rådighed stående takter fra styreenheden STW over de pågældende registre og andre komponentgrupper bliver de til den ønskede tidsselektion ved senderen og modtageren nødvendige tidsvinduer automatisk indstillet. Sendesidens tidsvindue for udsendelse af en burst er i fig. 2 betegnet med ZF-SB. Selve bursten består på indgangssiden af tidssignaldelen ZC og de efterfølgende afsnit i form af informationsdelen IN og fejlsikringsdelen EDC.

Det øverste diagram i fig. 2, som er betegnet med BS, er tilknyttet den bursten Be sendende station. Det nederste med Be betegnede tidsdiagram er tilknyttet den bursten Be modtagende station. Den bursten sendende station bliver i tilslutning til tidsvinduet ZF-SB under tidsintervallet UZ omkoblet fra udsendel-

se til modtagelse. For den på den modtagende station efter løbetiden LZ ankommende burst findes tidsvinduet ZF-EB, der imidlertid som følge af den ukendte løbetid er valgt tilsvarende større end tidsvinduet ZF-SB.

På den bursten Be modtagende station bliver der i tilslutning til modtagelsen af bursten skiftet fra modtagelse til udsendelse i tidsintervallet UZ, og derpå udsendes inden for tidsvinduet ZF-SRQ kvitteringssignalet RQ. Efter løbetiden LZ ankommer kvitteringssignalet på den bursten sendende station, og det kan dér modtages inden for tidsvinduet ZF-ERQ for modtagelse af kvitteringssignalet.

På den bursten modtagende station er der endvidere til erkendelse af en tidssignal-korrelationsspids indtegnet et tidsvindue ZF-KS, ved hjælp af hvilket muligheden for en fejlalarm ligeledes begrænses væsentligt. Tidsvinduet for tidssignal-korrelationsspidsen ZF-KS skal være valgt så bredt, at tidssignal-korrelationsspidsen også under hensyntagen til den ikke kendte løbetid samt en maksimal urtolerance ligger éntydigt i dette tidsvindue.

Det i fig. 3 viste blokdiagram over en sende-modtagestation til kontinuerlig signaldrift adskiller sig kun i detaljer fra blokdiagrammet i fig. 1, således at beskrivelsen deraf kan begrænses til disse detaljer. Styreenheden har her en yderligere taktudgang H og to yderligere styresignalindgange m og n. Disse yderligere tilslutninger er nødvendige til et matrikslager MSP, som skal forklares nærmere, og som forefindes i stedet for regeneratoren RR i fig. 1, og til en yderligere opkaldtæller RZ.

Som følge af de meget nøjagtige stationskvartsure QH er det også ved drift med kontinuerlige signaler sikret, at chiffreringsudstyret på to stationer, der vil træde i forbindelse med hinanden, hele døgnet allerede er så vidtgående synkrone, at de kan opbygge en forbindelse inden for et såkaldt "rendezvous-vindue".

Et sådant vindue bliver f.eks. kun indstillet hvert andet sekund. Ved indstilling af kaldenummeret for den ønskede abonnentstation på den kaldende station ved hjælp af kaldenummergiveren NG afgives først en kaldeburst Br, som udgør et selektivopkald, og som omfatter et en barkerkode udgørende tidssignal ZC og en chiffreringsfølge SF, og som udsendes på en frekvens, på hvilken den modtagende station modtager kaldebursten. Kaldesignalet er ligesom tidssignalet, der udgør en barkerkode, fast koblet i dataregistret D-RG. Ved begyndelsen af en kaldeburst tilføres først over omskifteren U3 i koblestilling 2 og omskifteren U2 i koblestilling 1 tidssignalet umiddelbart til senderen S på uchiffreret form. Derefter bliver omskifteren U3 bragt i koblestillingen 1, og samtidigt bliver det eksempelvis af 36 ét'er bestående kaldesignal i dataregistret D-RG og chiffreringsfølgen i chiffreringsregistret S-RG tilført chiffreringsapparatet AD. Det chiffrerede kaldesignal bliver over omskifteren U3 og omskifteren U2 ligeledes tilført senderen S, som udstråler hele kaldebursten over sende-modtageomskifteren U1 og antennen A.

Den på den fjerne station ankommende kaldeburst Br bliver over sende-modtageomskifteren U1 med koblearmen i den med punkterede linier tegnede koblestilling tilført modtageren E, som på udgangssiden er forbundet med tidssignal-korrelatoren ZZ-K. Tidssignal-korrelationsspidsen, der markerer erkendelsen af tidssignalet, bliver til korrektion af modtagesidens taktfase tilført taktudnyttelsen TA, som for sit vedkommende tilfører matrikslageret MSP takten i den korrigerede taktfase og på denne måde foranlediger matrikslageret MSP til at tilføre det efter tidssignalet følgende kaldesignal umiddelbart til dechiffreringsapparatet SU. Dechiffreringsapparatet SU dechiffrerer kaldetegnet ved hjælp af den fra chiffreringsregistret S-RG tilførte chiffreringsfølge og leverer på udgangssiden kaldesignalet til opkaldtælleren RZ. Hvis opkaldtælleren

RZ af de mulige 36 ét'er tæller mindst 32 ét'er, signalerer den dette til styreenheden STW over styresignalindgangen n. Styreenheden STW foranlediger for sit vedkommende, at kvitteringssignalet fra kvitteringssignalregistret RQ-RG i en nøjagtigt defineret tidsafstand fra den i tidssignal-korrelatoren ZZ-K optrædende tidssignal-korrelationsspids over omskifteren U4 og omskifteren U2 i koblestillingen 2 tilføres senderen S og udstråles over sende-modtageomskifteren U1 og antennen A.

Denne fast forudgivne tidsmæssige afstand mellem tidssignal-korrelationsspidsens optræden på modtagesiden og udsendelsen af kvitteringssignalet RQ gør det muligt for den kaldebursten udsendende station at konstatere radioløbetiden og på grundlag af dette kendskab nu at indstille et nøjagtigt tidsvindue for modtagelsen af det kvitteringssignal, der som reaktion på hver nu udsendte informationsburst sendes tilbage fra den fjerne station.

Så snart den kaldebursten sendende station har modtaget kvitteringssignalet, som kvitterer for modtagelsen af opkaldet på den opkaldte station, skifter styreenheden STW fra opkald til drift. Ca. hver 300 ms bliver der nu til en ny informationsburst frembragt en ny chiffreringsfølge. Den af den chiffrerede information inklusive fejlsikring bestående informationsburst bliver over omskifteren U3 i koblestilling 1 og omskifteren U2 tilført senderen S, som udstråler den over sende-modtageomskifteren U1 og antennen A til den fjerne station.

På den fjerne station bliver informationsbursten over sende-modtageomskifteren U1 med koblearmen i den med punkterede linier tegnede koblestilling igen tilført modtageren E, som på udgangssiden videregiver informationsbursten til det allerede nævnte matrikslager MSP. I matrikslageret MSP bliver alle ankommende informationsbit lagret i eksempelvis otte faser i en matriks. Derpå konstateres det over udnytteren AW, i

hvilke på hinanden følgende bitfasespalter det mindste antal bitspringovergange optræder, og denne overgang henholdsvis disse overgange signaleres da til taktudnyttelsen TA til fastlæggelse af modtagesidens taktfase. Den i en således markeret bitfasespalte i matrikslageret MSP lagrede informationsburst bliver nu viderebearbejdet på den allerede i forbindelse med stationskoblingen i fig. 1 beskrevne måde.

Som det blev nævnt indledningsvis, tillader anvendelsen af matrikslageret på denne måde en udligning af løbetidsvariationer på indtil 1/2 bit. Hvis også løbetidsvariationer > 1/2 bit skal kunne udlignes, er dette muligt ved, at de otte bitfasespalter dechiffreres efter hinanden og tilføres fejlsikringen. Fastlæggelsen af modtagesidens taktfase sker nu ved hjælp af en af modtageren til informationsafgivelse sluttelig også modtaget bitfasespalte, som er fejlfri henholdsvis korrigerbar. I fig. 3 er dette alternativ antydet ved anbringelse af udnytteren AW (punkteret linie) i forbindelse med fejlsikringen FS.

Ved hjælp af de kun til bestemte tidspunkter til rådighed stående takter fra styreenheden STW over de hertil forhåndenværende registre og andre komponentgrupper bliver også her de til den ønskede tidsselektion i senderen og modtageren nødvendige tidsvinduer indstillet automatisk. Til nærmere forklaring af denne tidsvindueteknik er der på lignende måde som i fig. 2 vist tidsdiagrammer i fig. 4 for opkaldfasen og i fig. 5 for den normale drift.

Som tidsdiagrammet BS i fig. 4 viser, bliver den af tidssignalet ZC og chiffreringsfølgen SF bestående kaldeburst Br udsendt inden for tidsvinduet ZF-SB. I tilslutning dertil skiftes der i tidsintervallet UZ fra udsendelse til modtagelse. Ved afslutningen af løbetiden LZ ankommer kaldebursten Br, som tidsdiagrammet BE i fig. 4 viser, på den fjerne station, som hertil har indstillet et forholdsvis bredt tidsvindue ZF-ZC for modtagelsen af tidssignalet ZC.

Når tidssignal-korrelatoren ZZ-K i fig. 3 erkender tidssignalet ved optræden af tidssignal-korrelationsspidsen KS, begynder derfra den tid at gå, som er bestemmende for sendetidspunktet for kvitteringssignalet RQ. Dette tidsinterval er i diagrammet BE betegnet med ZT. Efter modtagelse af kaldebursten Br og erkendelse af tidssignal-korrelationsspidsen KS skifter stationen i tidsrummet UZ fra modtagelse til udsendelse og sender da kvitteringssignalet RQ inden for tidsvinduet ZF-SRQ. Kvitteringssignalet RQ ankommer efter løbetiden LZ på den kaldebursten sendende station og bliver der, som diagrammet BS viser, modtaget i et forholdsvis bredt tidsvindue ZF-ERQ' til modtagelse af kvitteringssignalet.

Som følge af den definerede udsendelse af kvitteringssignalet i en forudbestemt afstand fra tidssignal-korrelationsspidsen KS i det modtagne tidssignal på den opkaldte station har den kaldebursten udsendende station mulighed for, ud fra tidspunktet for modtagelse af kvitteringssignalet at bestemme løbetiden, og den kan således indstille et snævert tidsvindue for de kvitteringssignaler RQ, der tilbageoverføres fra den modtagende station i rytme med de informationsburster Bi, der nu skal udsendes. Dette forhold er vist i fig. 5. Informationsbursten Bi består i hvert enkelt tilfælde af informationsdelen IN og fejlsikringen EDC. Så snart informationsbursten er blevet modtaget på den fjerne station i tidsvinduet ZF-EB, som diagrammet BE i fig. 5 viser, sker omkoblingen fra modtagelse til udsendelse i tidsintervallet UZ og i tilslutning dertil udsendelsen af kvitteringssignalet RQ i tidsvinduet ZF-SRQ. Det efter løbetiden LZ på den informationsbursten sendende station ankommende kvitteringssignal RQ modtages i det nu snævre tidsvindue ZF-ERQ.

Den i fig. 6 viste tabel, der tjener til nærmere forklaring af virkemåden af matrikslageret MSP i fig. 3, går af hensyn til overskueligheden ud fra, at infor-

mationsbursten kun har otte bit, som aftastes i otte faser. Informationsbursten bliver altså med andre ord lagret i otte på hinanden følgende bitfasespalter, hvorhos den første ankommende bit i hvert enkelt tilfælde er placeret på tabellens øverste lagerplads og hver yderligere bit på en derunder liggende lagerplads. I linien A-Nr er de otte bitfaser 1, 2, 3 ... 8 angivet. Hvert binære ét er betegnet med et 1 og hvert binære nul er betegnet med et 0. Som det let ses, fremkommer der ved overgangen fra bitfasespalte 1 til bitfasespalte 2 fem bitspring og ved overgangen fra bitfasespalte 2 til bitfasespalte 3 seks bitspring osv. Antallene af bitspring fra overgang til overgang er angivet i linie W/Sp. Det viser sig, at der ved overgangene mellem bitfasespalterne 5 og 6 på den ene side og mellem bitfasespalterne 6 og 7 på den anden side ikke optræder bitspring, og at derfor midten af dette med "Opt.-fase" betegnede bitfasespalteområde markerer den søgte rigtige taktfase på modtagesiden.

P A T E N T K R A V

1. Fremgangsmåde til sikret overføring af digitale signaler, navnlig data via kortbølge, hvor de med en datasikring forsynede chiffrerede signaler overføres blokvist (burst) fra en sende- til en modtagestation, og hvor der fra modtagestationen før udsendelse af en yderligere burst tilbageoverføres et kvitteringssignal til sendestationen (automatic request), k e n d e t e g n e t ved, at synkroniseringen mellem to stationer i forbindelse med præcisionskvartsure, som findes på stationerne, tilvejebringes ved hjælp af et i det mindste ved begyndelsen af en signaloverføring sendt tidssignal i form af en kodebølge med gode autokorrelationsegenskaber, som kan udnyttes på modtagesiden i en tidskanal-korrelator (ZZ-K) til efterstyring af modtagesidens taktfase, at endvidere sende- henholdsvis modtagefrekvensen i frekvensspringintervaller, som omfatter udsendelse af en burst og modtagelse af kvitteringssignalet fra den fjerne station, ændres pseudotilfældigt inden for rammerne af et forudbestemt frekvenskollektiv og herved chiffreringsfølgen for chiffreringen af en burst og af det tilhørende kvitteringssignal samt til fremstilling af en frekvensadresse nyberegnes for hver burst på grundlag af stationskvartsurets urtid og den bursten modtagende stations kaldenummer, og at bursten i forbindelse med en upåklagelig modtagerefererende chiffrering på modtagesiden samtidigt tjener til adressering og til identifikation ved, at kun en med den rigtige kode dechiffreret og som fejlfri henholdsvis fejlkorrigeret erkendt burst modtages af modtageren.

2. Fremgangsmåde ifølge krav 1 til overføring af signalinformationer, der hver især er begrænset til en burst, k e n d e t e g n e t ved, at hver enkeltburst (Be) omfatter en chiffreret informationsdel (IN), en chiffreret fejlsikringsdel (EDC) og en foran disse to

dele stillet uchiffreret tidssignaldel (ZC).

3. Fremgangsmåde ifølge krav 1 til overføring af en signalinformation, som omfatter et antal burster, k e n d e t e g n e t ved, at der foran den informationsburst (Bi), der skal overføres, og som omfatter en chiffreret informationsdel (IN) og en chiffreret fejlsikringsdel (EDC), sættes en kaldeburst (Br), som omfatter et tidssignal (ZC) og en chiffreringsfølge (SF), der udgør selektivkaldet, hvilken kaldeburst efter modtagelse og erkendelse af opkaldet på den modtagende station bevirker udsendelse af kvitteringssignalet med en fast forudbestemt tidsafstand (ZT) i relation til det modtagne tidssignal, og at der ud fra modtagesiden for dette kaldebursten (Br) kvitterende kvitteringssignal (QR) på den kaldende station indstilles et snævert tidsvindue (ZF-ERQ) til modtagelse af yderligere kvitteringssignaler i forbindelse med den efterfølgende overføring af informationsburster.

4. Fremgangsmåde ifølge krav 1 og 3, k e n d e t e g n e t ved, at hver ankommende bit i en informationsburst (Bi) på modtagesiden før dechiffreringen indlæses i flere faser, f.eks. otte faser, i et matrikslager (MSP), at der endvidere over en bestemmelse af de bitfasespalter, der udmærker sig ved et mindsteantal af bitspringovergange, foretages en fastlæggelse af modtagesidens taktfase til midten af dette bitfasespalteområde, og at derpå den til denne taktfase knyttede bitfasespalte dechiffreres og tilføres fejlsikringen (FS).

5. Fremgangsmåde ifølge krav 1 og 3, k e n d e t e g n e t ved, at hver ankommende bit i en informationsburst (Bi) på modtagesiden først indlæses i flere faser, f.eks. otte faser, i et matrikslager (MSP) og derpå hver bitfasespalte dechiffreres og tilføres fejlsikringen (FS), og at der til fastlæggelse af modtagesidens taktfase bestemmes en af modtageren til informationsafgivelse sluttelig også antaget bitfasespalte, som er fejlfri henholdsvis fejlkorrigerbar.

6. Fremgangsmåde ifølge et eller flere af de foregående krav, k e n d e t e g n e t ved, at tidsintervallet mellem to på hinanden følgende sendetidspunkter for udsendelse af en burst ændres pseudotilfældigt inden for forudbestemte grænser ved hjælp af chiffreringsudstyret.

FIG 1

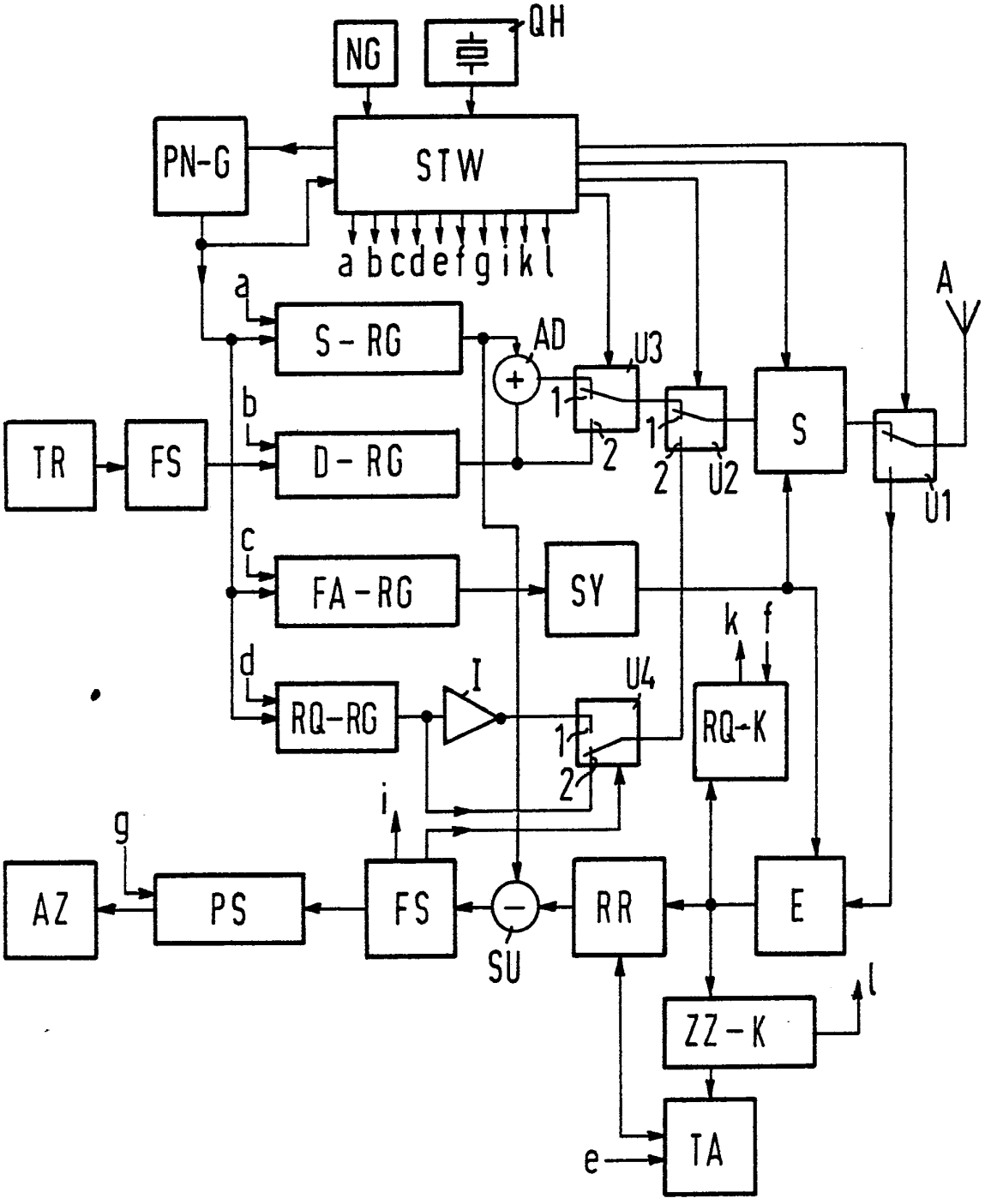

NG
QH
PN-G
STW
a b c d e f g i k l
a
S - RG
AD
U3
A
b
TR
FS
D - RG
1
2
S
U2
U1
c
FA - RG
SY
k f
d
RQ-RG
I
U4
RQ-K
i
g
AZ
PS
FS
SU
RR
E
l
ZZ - K
TA
e

FIG 2

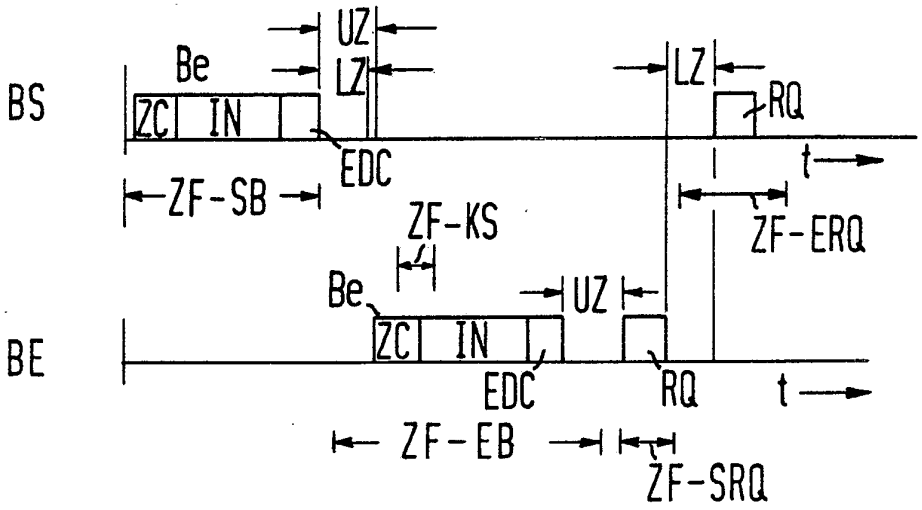


FIG 4

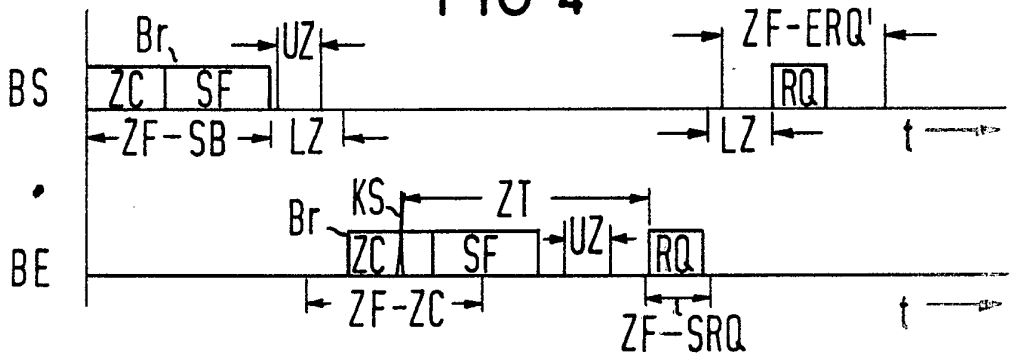


FIG 5

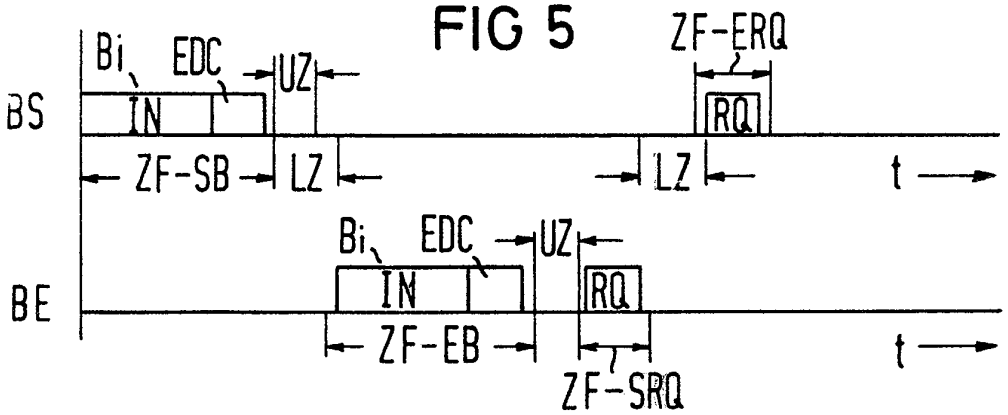


FIG 3

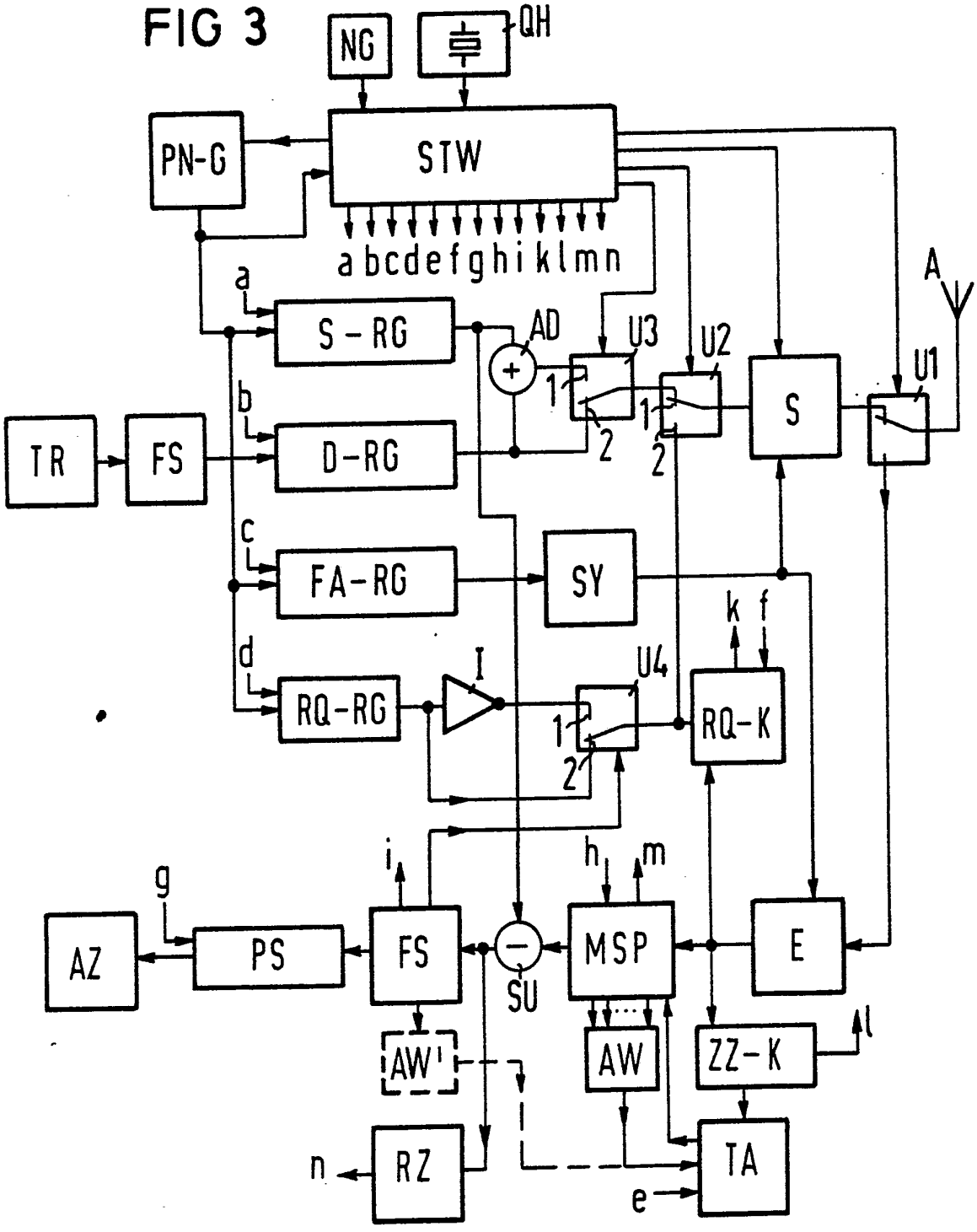
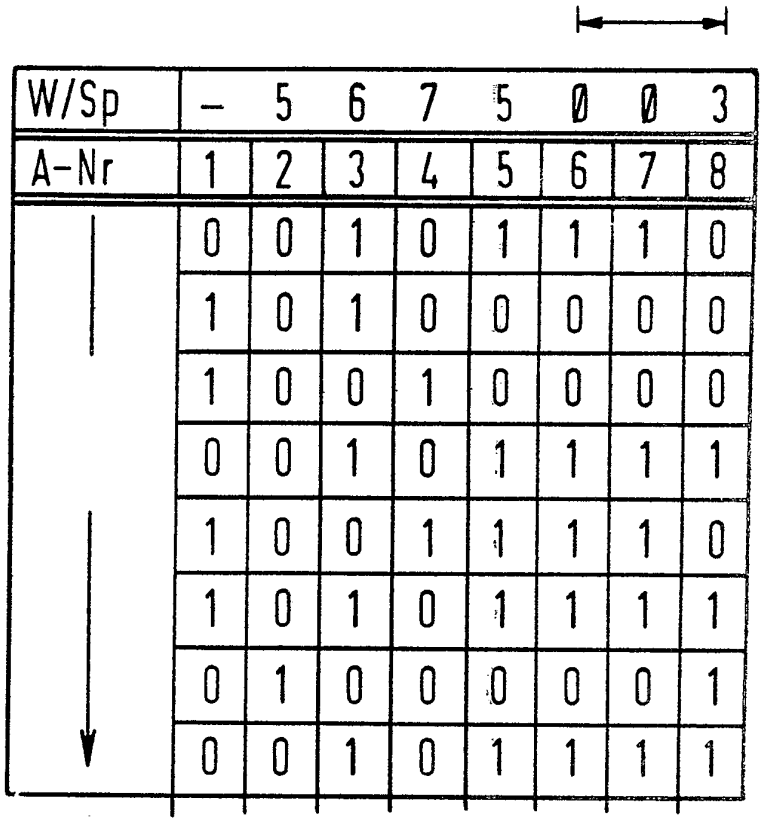

NG
QH
PN-G
STW
a b c d e f g h i k l m n
A
a
S - RG
AD
U3
U2
U1
S
b
TR
FS
D-RG
c
FA-RG
SY
k f
d
RQ-RG
I
U4
RQ-K
i
h
m
g
AZ
PS
FS
SU
MSP
E
AW'
AW
ZZ-K
l
n
RZ
TA
e

FIG 6



W/Sp	–	5	6	7	5	Ø	Ø	3
A-Nr	1	2	3	4	5	6	7	8
	0	0	1	0	1	1	1	0
	1	0	1	0	0	0	0	0
	1	0	0	1	0	0	0	0
	0	0	1	0	1	1	1	1
	1	0	0	1	1	1	1	0
	1	0	1	0	1	1	1	1
	0	1	0	0	0	0	0	1
	0	0	1	0	1	1	1	1