NORGE
[NO]

STYRET
FOR DET INDUSTRIELLE
RETTSVERN

[B] (11) **UTLEGNINGSSKRIFT** Nr. 137802

(51) Int. Cl.² H 04 K 1/02

(21) Patentsøknad nr. 3984/73
(22) Inngitt 15.10.73
(23) Løpedag 15.10.73

(41) Alment tilgjengelig fra 12.01.76
(44) Søknaden utlagt, utlegningsskrift utgitt 16.01.78

(30) Prioritet begjært 23.11.72, Forbundsrepublikken Tyskland, nr. P 22 57 361

(54) Oppfinnelsens benevnelse Overføringssystem.

(71)(73) Søker/Patenthaver SIEMENS AKTIENGESELLSCHAFT
BERLIN UND MÜNCHEN,
Hofmannstrasse 51,
D-8000 München 25,
Forbundsrepublikken Tyskland.

(72) Oppfinner ERICH METZGER, München,
FRANZ MOTYKA, Fürstenfeldbruck,
Forbundsrepublikken Tyskland.

(74) Fullmektig Siv.ing. Per Onsager,
Onsagers Patentkontor, Oslo.

(56) Anførte publikasjoner Ingen.

137802

Oppfinnelsen angår et overføringssystem som består av et sendested og et eller flere mottagningssteder og tjener til å formidle chifrerte informasjoner, og hvor der i sendestedet er anordnet et apparat som forarbeider klarsignalet, og et chifreringsapparat (koder og nøkkelgenerator), mens der på mottagningsstedet foruten et dechifreringsapparat (dekoder og nøkkelgenerator) også er anordnet et klartekstapparat, samt hvor der fra sende-siden til mottagnings-siden formidles informasjoner (innstillingssignaler) til innstilling av synkronismen mellem koder og dekoder.

F.eks. ved informasjonsoverføring i simpleks-drift, d.v.s. en metode hvor informasjonsstrømmen går ensidig fra et sendested til et eller flere mottagningssteder og enhver forbindelse i motsatt retning mangler, melder der seg i tilfellet av anvendelsen av chifreringsinnretninger som arbeider med kvasi-tilfeldighetsgeneratorer, det problem å tilveiebringe eller gjenopprette synkronismen mellem nøkkelgeneratorene på sende- og mottagningssiden. I denne forbindelse skal det nevnes at nøkkelgeneratorene ved slike innretninger kan innstilles fritt velgbart med hensyn til en nøkkelsignalsekvens som frembringes i dem, ved hjelp av ekstra informasjonsbærere som hullkort o.l., så sekretessen til tross for nøkkelgeneratorens innstilling, som eventuelt kan konstateres i overføringen, blir sikret på betryggende måte ved hyppig skiftning av forhåndsinnstillingen.

De kjente chifrerings- og dechifrerings-innretninger er vanskelige å ha å gjøre med i praksis fordi de ikke kan samarbeide med vilkårlige klartekstapparater. For klartekstapparatene må være utformet slik at de tillater den ved chifreringsapparatet bestemte innblending av nøkkelgeneratorens innstilling; det måtte da være om man tillot en delvis undertrykkelse av den informasjon som skal overføres.

Til grunn for oppfinnelsen ligger den oppgave å bli uavhengig nettop når det gjelder dette krav, så det blir mulig innen vide grenser å la vilkårlige klartekstapparater samarbeide med et chifreringsapparat. Denne oppgave blir ved en innretning av den innledningsvis omtalte art ifølge oppfinnelsen løst ved at der i det enkelte mottagningssteds klartekstapparat er anordnet en innretning til å konstatere en feilaktig dechifrering, og at denne innretning, når kriteriet for defekt dechifrering opptrer, bringes til å forårsake en nyinnstilling av dekoderens nøkkelgenerator på grunnlag av innstillingssignaler innblendet i det mottatte signal.

I det følgende vil oppfinnelsen bli belyst nærmere ved et utførelseseksempel.

Tegningen viser på fig. 1 et system til chifrert formidling av informasjoner mellem et sendested og et mottagningssted. Ved simpleksdrift kan der istedenfor dette ene mottagningssted også benyttes flere mottagningssteder adskilt fra hverandre i rommet, og hvert av disse mottagningssteder kan være utført som det viste. Figuren er ennvidere tegnet som blokk-koblingsskjema, da de enkelte koblingsblokker inneholder apparatur i henhold til tidligere kjent teknikk.

Det viste system skal f.eks. tjene til formidling av flere telefonsamtaler, noe som på tegningen er antydet ved kanaltilslutninger K1, K2 ..... Kn på inngangssiden og kanaltilslutninger K1', K2' .... Kn' på utgangssiden. Tilslutningene fører på sendesiden til et klartekstapparat 15 og kommer på mottagningssiden fra et klartekstapparat 20. Videre er det forutsatt at det dreier seg om et overføringssystem som arbeider med pulskodemodulasjon i klartekstapparatene 15 og 20. I tillegg er systemet også utformet for drift efter tidsmultiplekspринsippet, slik det i og for seg er blitt vanlig ved PCM-forbindelser. De enkelte kanalinnganger fører i klartekstapparatet på sendesiden til en analog-digitalomformer 1 som forsynes med bit-takten fra en taktsentral 2. Taktsentralen 2 leverer dessuten bit-takten til rammepulsgeneratoren 3, som i sin tur forsyner analog-digitalomformeren 1 med de nødvendige rammesynkrontegn. Denne teknik er alminnelig kjent ved PCM-overføringsinnretninger og vil derfor forsåvidt ikke bli forklart nærmere. F.eks. er denne teknikk utførlig beskrevet i publikasjonen "Die Pulscode-Modulation und ihre Anwendung in Fernmeldewesen", Jahrbuch des elektrischen Fernmeldewesens, 19 (1968), side 184 - 242, og den litteratur som der henvises til der. Det binære klartekstsignal KTS blir tilført chifreringsapparatet 16, som omfatter den egentlige

koder 4, f.eks. et modulo-2-addisjonsapparat, nøkkelgeneratoren 5 og en synkrontegninnretning 6 samt en omkobler 7. Klartekstsignalet KTS blir direkte tilført koderen 4, som overlagrer dette signal med den binære nøkkelsignalfrekvens fra nøkkelgeneratoren 5 og avgir det chifrerte binærsignal GTS ved sin utgang. I chifreringsapparatet innmates dessuten også taktsignalet T og fra rammesynkrongeneratoren 3 det sendesidige synkroniserings-kommandosignal SynS (senere også betegnet som styresignal), som fortrinnsvis avgis i tidsavstander svarende til et helt multiplum av PCM-rammeperioden. Rammesynkroniseringssignalet SynS blir herunder tilført synkroniseringsinnretningen 6, som også får tilført enten den respektive innstilling eller et tilsvarende signal fra nøkkelsignalgeneratoren 5. Den innstilling som tilsvarer det respektive øyeblikk under drift, blir i chifreringsteknikken også ofte betegnet som tellerstand.

Fra utgangen fra koderen 4 blir det binære chifrerte signal GTS tilført den ene tilslutning til omkobleren 7, hvis annen inngangstilslutning er forbundet med en utgang for synkroniseringsinformasjonen fra innretningen 6. Fra utgangstilslutningen til omkobleren 7 forsynes strekningsapparatet 17. Strekningsapparatet 17 på sendesiden har til oppgave å bringe det binære chifrerte signal GTS på en form som egner seg for overføringen (enten det nu er med hensyn til amplitude eller fase, altså alt efter modulasjonsform). Istedenfor strekningsapparatet kan der eventuelt også benyttes en direkte gjennemgående forbindelse til mottagningssiden. Vanlige strekningsapparater på sendesiden utgjøres f.eks. av senderen for en retningsradiostrekning eller fasemodulatoren for en radiostrekning eller ledningsapparatdelen for en ledningsforbindelse etc. Fremfor alt hvis strekningsapparatet er utformet for å arbeide med pulsmodulasjon, er det å anbefale i tillegg (som også vist) å forsyne strekningsapparatet 17 med en bit-takt-synkronisering.

Overføringssystemets mottagningsside begynner i utførelseseksempelet likeledes med et strekningsapparat 18, og for dette gjelder det samme som ble sagt med hensyn til strekningsapparatet 17 på sendesiden. Da det i utførelseseksempelet er antatt at innretningen arbeider med binærsignaler, er der i strekningsapparatet 18 på mottagningssiden anordnet en taktgjenvinningskobling 18' som stiller bit-taktsignalet T til rådighet. Ved utgangen fra strekningsapparatet 18 fås det chifrerte binære signal GTE som tilsvarer det chifrerte signal GTS på sendesiden. Dette chifrerte signal blir i dechifreringsapparatet 19 tilført dekoderen 8. Denne er analogt med sendesiden likeledes et modulo-2-

addisjonsapparat. Modulo-2-addisjonsapparatet 8 får den binære nøkkelsignalsekvens fra en nøkkelgenerator 9, som er utført tilsvarende nøkkelgeneratoren 5 på sendesiden og ved samme startinnstilling frembringer et signal maken til det fra nøkkelgeneratoren 5. Ved riktig virkemåte av nøkkelgeneratoren 9 foreligger derfor ved utgangen fra dekoderen 8 det binære klartekstsignal KTE som stemmer overens med det binære klartekstsignal KTS på sendesiden. Det binære klartekstsignal KTE blir tilført en digital-analog-omformer 10 som befinner seg i klartekstapparatet 20 på mottagningssiden, og som tilsvarer den vanlige kodeomformer i et PCM-system og ved sine utganger K1', K2' .... Kn' stiller signalene for de n kanaler til rådighet.

Med bit-taktsignalet T forsynes foruten dekoderen 8, nøkkelgeneratoren 9 og digital-analog-omformeren 10 også to ytterligere koblingsgrupper 11 og 12. Koblingsgruppen 11 omfatter foruten en rammepulsgenerator tilsvarende rammepulsgeneratoren 3 på sendesiden også en rammepuls-overvåkningskobling. Ennvidere inneholder den en innretning som forårsaker en omkobling av bryteren 13 når det i 11 er konstatert at rammepulsene ikke blir riktig identifisert i det binære klartekstsignal KTE. Koblingsgruppen 12 inneholder en tydningskobling som uttar den på sendesiden innblendede synkroninformasjon, fremfor alt tellerstanden ved 5, fra det chifrerte mottatte binære signal GTE og forårsaker en tilsvarende nyinnstilling av nøkkelgeneratoren 9. Ved hjelp av bryteren 13 blir det sikret at denne nyinnstilling av nøkkelgeneratoren 9 bare skjer når rammesynkroniseringen i det binære klartekstsignal KTE ikke er riktig identifisert i 11.

Til ytterligere forklaring av utførelseseksempelet på fig. 1 viser fig. 2 tidsdiagrammer for de funksjoner som er vesentlige for forløpet av en synkroniseringsprosess. Pulstoget A representerer synkroniserings-kommandosignalet SynS, som fra rammegeneratoren 3 i 15 på sendesiden avgis til koderen 16, og som fortrinnsvis utsendes i jevne tidsavstander a svarende til et helt multiplum av PCM-rammeperioden. Signalet SynS bevirker hver gang ved omstyring av bryteren 7 innblending av synkroniseringstegn fra synkroniseringsinnretningen 6 i den chifrerte tekst GTS som avgis til 17, og som på fig. 2 er vist som signal B. Efter slutten av hver synkrontegnsekvens, hvis varighet er betegnet med b, blir bryteren 7 ved hjelp av synkroniseringsinnretningen 6 selv igjen styrt tilbake til normalstilling.
C på fig. 2 betegner det styresignal SynE som på mottagningssiden avgis fra den i 20 inneholdte synkronovervåkning 11 til bryteren 13. I den

forbindelse skal det antas at det på tidspunktet c er konstatert i koblingsdelen 11 at synkronismen av dechifreringen er gått tapt. Fra tidspunktet c av er synkronkoblingen 12 parat til å tyde synkroniserings-tegn som ankommer via bryteren 13 og er innblendet i GTE, og å bevirke en innstilling av nøkkelgeneratoren. Første gang efter tidspunktet c blir synkroninformasjonen e, som er vist uttrukket ved D på fig. 2, tydet. I det viste eksempel skal det antas at synkroniseringsforsøket ved e ble uten resultat, f.eks. fordi overføringsfeil hadde bevirket at det foranstillede Barker-kode-signal ikke var konstatert. I dette tilfelle foretas neste synkroniseringsforsøk ved f. Fører dette frem, så har koblingsdelen 11 på tidspunktet d konstatert at synkronismen mellem nøkkelgeneratorene er gjenopprettet. Det av 11 avgitte kriterium SynE forsvinner, og synkroniseringstyderen 12 blir ved hjelp av bryteren 13 igjen koblet fra GTE-ledningen.

Det viste overføringssystems virkemåte er som følger:

De analoge signaler ved kanaltilslutningene Kl - Kn blir i 1 omsatt til et PCM-signal. Dette PCM-signal inneholder også et rammesynkrontegn av vanlig slag. Det er et tidsmultiplekssignal KTS når det gjelder overføringskanalene Kl - Kn. Tidsmultiplekssignalet KTS blir i koderen 4 omsatt til det såkalte kryptogram GTS og via strekningsapparatet 17 gitt ut på overføringsstrekningen 21. Omkobleren 7, som normalt gir forbindelse mellem strekningsapparatet 17 og koderen 4, blir bragt til sin annen koblingsstilling og forbundet med synkroniseringen 6 enten i regelmessige tidsavstander, f.eks. efter hver annen eller tredje avsluttede pulsramme hos tidsmultiplekssystemet, eller til enhver tid bare på tidspunkter da der, betinget ved klarsignalet som skal overføres, finnes hull i informasjonsstrømmen. Disse hull forekommer følgelig også i signalet KTS. Synkroniseringsinnretningen 6 får som allerede nevnt meddelelse om den til enhver tid foreliggende koblingstilstand resp. tellerstand fra nøkkelgeneratoren 5 og avgir den via den tilsvarende tilslutningsledning til den tilsvarende tilslutning på omkobleren 7. I utførelseseksempelet er manøvreringen av omkobleren 7 vist slik at den skjer indirekte fra rammesynkrongeneratoren 3, nemlig på den måte at der i og med omstillingen av omkobleren 7 til dens nedre koblingsstilling tillike bevirkes et startsignal for synkroninnretningen 6 til å avgi tellerstanden hos 5. For å skaffe betryggende sikkerhet for innstilling av nøkkelgeneratoren 9 på mottagningssiden efter den nye tellerstand er det i den forbindelse å anbefale før utsendelsen av tellerstanden å bevirke utsendelse av et varslingstegn, f.eks. en pulssekvens efter

Barker-koden, så der over tilførselsledningen fra 6 til 7 først kommer en kort bit-sekvens i Barker-koden og først derpå tellerstanden ved 5.

På mottagningssiden blir dekoderen 8 matet med det mottatte kryptogram GTE og får det tilsvarende nøkkelsignal tilført fra nøkkelgeneratoren 9. Klarteksten KTE fås følgelig i binær form ved inngangen til digital-analog-omformeren 10 og blir av denne tilsvarende fordelt på kanalene Kl' - Kn' efter tidsmultiplekssprinsippet. Her står dermed signalet til rådighet i analog form. Digital-analog-omformeren 10 får i utførelseseksempelet taktfrekvensen resp. bit-taktsignalet tilført direkte fra mottagningssidens strekningsapparat 18, som i koblingsdelen 18' avleder taktsignalet fra de mottatte pulser. Det rammesynkronsignal som behøves for digital-analog-omformningen og den samtidige oppløsning av tidsmultipleksrammen, blir tilført digital-analog-omformeren 10 fra koblingsgruppen 11 og rammesynkrongeneratoren i denne. Rammesynkronsignalet fra 11 blir dessuten sammenlignet med det binære klartekstsignal som forekommer i KTE, nemlig i den koblingsdel som gjennemfører synkronovervåkningen i 11.

Stemmer det mottatte rammesynkronsignal overens med det rammesynkronsignal som frembringes på mottagningssiden, så skjer der ikke noe mer, idet dechifreringen kan antas å være korrekt. Men er dette ikke tilfellet, d.v.s. hvis det rammesynkronsignal som frembringes på mottagningssiden, og det lemlestede eller ikke lenger identifiserbare rammesynkronsignal som forekommer i KTE, ikke stemmer overens, blir bryteren 13 som antydet bragt til sin nedre koblingsstilling og tydningskoblingen 12 koblet til utgangen fra 18 og dermed til den ledning som inneholder det i binær form foreliggende kryptogram. Synkron-tydningskoblingen 12 inneholder en første koblingsenhet som reagerer når varseltegnet resp. det nevnte Barker-kode-signal mottas, og forbereder opptagelse av tellerstanden som følger efter varselsignalet. Blir tellerstanden så mottatt, gir koblingsgruppen 12 denne tellerstand direkte videre til nøkkelgeneratoren 9 og innstiller denne pånу. Da dekoderen 8 er tilkoblet utgangen fra 18 til stadighet, opptrer så i utgangen fra 8, når nøkkelgeneratoren 9 er riktig innstillet ved hjelp av tydningskoblingen 12, det binære klartekstsignal KTE i korrekt form. Det betyr med andre ord at de rammesynkrontegn som inneholdes i dette signal, igjen stemmer overens med dem som frembringes i mottageren. I denne tilstand blir bryteren 13 automatisk bragt i sin annen øvre koblingsstilling og tydningskoblingen 12 skilt fra.

Synkrontegnene med forutgående varselsignal, eksempelvis

Barker-kode-signal, behøver ikke å innblendes i det fra sende- til mottagnings-side overførte kryptogram til stadighet. I tilfellet av en forhåndenværende returforbindelse fra mottagningsstedet til sendestedet er det også mulig via den stiplet antydede overføringsforbindelse 14 å gi sendestedet en kravinformasjon for utsendelse av synkrontegnene resp. tellerstanden. Denne utkrevningsteknikk er i og for seg tidligere kjent fra DOS 2.017.282, så det ikke er nødvendig å gå nærmere inn på den her.

Det beskrevne overføringssystem har fordelen av ekstremt liten ømfintlighet for forstyrrelser, også når det gjelder tilsiktet forstyrrelse fra fremmed hold. En nyinnstilling av nøkkelgeneratoren 9 på mottagningssiden skjer nemlig til enhver tid først når klartekstapparatet på mottagningssiden har konstatert manglende overensstemmelse i rammesynkroniseringen av klarteksten.

En vesentlig fordel ved det beskrevne system er imidlertid fremfor alt å se i at vilkårlige klartekstapparater kan samarbeide med chifrerings- og dechifrerings-apparatene 16 og 19, såfremt klartekstapparatene 20 på mottagningssiden er forsynt med en utgang SynE som gjør det mulig å konstatere at rammesynkroniseringen eller et annet kjennetegn som efter avtale er innføyet i overføringen av klarteksten, mangler eller er forstyrret, og såfremt klartekstapparatene 15 på sendesiden har en utgang SynS som avgir et signal hvorfra det kan utledes på hvilket tidspunkt nøkkelapparatet 16 til enhver tid skal innblende synkroninformasjoner i kryptogramstrømmen GTS. I utførelseseksempelet ytrer dette seg ved at koblingsgruppene 15 og 20 er vist som separate komponenter i forhold til kryptografkomponentene 16 på sendesiden og 19 på mottagningssiden.

P a t e n t k r a v :

1. Overføringssystem som består av et sendested og et eller flere mottagningssteder og tjener til overføring av chifrert informasjon, og hvor der på sendesiden er anordnet et apparat som forarbeider klarsignalet, og et chifreringsapparat (koder og nøkkelgenerator) tilkoblet dette apparat, mens der på det enkelte mottagningssted foruten et dechifreringsapparat (dekoder og nøkkelgenerator) også er anordnet et klartekstapparat, samt hvor der fra sendesiden til mottagningssiden formidles informasjoner (innstillingssignaler) for synkron innstilling av koder og dekoder, k a r a k t e r i s e r t ved at der i klartekstapparatet på det enkelte mottagningssted er anordnet en innretning (11) til å konstatere en feilaktig dechifrering, og at denne innretning

(11) ved opptreden av kriteriet for mangelfull dechifrering bevirker en nyinnstilling av dekoderens (8) nøkkelgenerator (9) på grunnlag av innstillingssignaler innblendet i det mottatte signal (GTE).

2. Overføringssystem som angitt i krav 1, k a r a k t e r i s e r t ved at klartekstapparatet (15) på sendesiden inneholder en analog-digital-omformer (1), særlig efter PCM-teknikkens prinsipp, som i regelmessige tidsavstander innblender synkronsignaler, eksempelvis rammesynkronsignaler, i den digitale klartekst (KTS), og at klartekst-apparatet (20) på mottagningssiden inneholder en digital-analog-om-former (10) forsynt med en kobling (11) som tjener til å avføle synkronsignalene, og som ut fra en feilaktig mottagning av synkronsig-nalene i den dechifrerte digitale klartekst (KTE) avleder kriteriet for konstatering av en mangelfull dechifrering.

3. Overføringssystem som angitt i krav 1 eller 2, k a r a k t - e r i s e r t ved at en nyinnstilling av den respektive dekoder (8) på mottagningssiden først bevirkes ved flere gangers feilaktig mot-tagning av de i klarteksten (KTE) inneholdte synkrontegn (drift med en som tillatelig vurdert feilandel, f.eks 10^{-4} og bedre).

4. Overføringssystem som angitt i et av kravene 1 - 3, k a r a k t e r i s e r t ved at der på sendesiden før overføringen av det egentlige innstillingssignal for dekoderne (8) på mottagnings-siden hver gang overføres et varselsignal, f.eks. et signal efter Barker-koden.

5. Overføringssystem som angitt i et av kravene 1 - 4, k a r a k t e r i s e r t ved at der i systemet som i og for seg kjent er anordnet en returforbindelse (14) (fra det enkelte mottag-ningssted til sendestedet), og at utsendelsen av informasjoner (inn-stillingssignal) for synkroninnstillingen av koder (4) og dekoder(8), på i og for seg kjent måte aktivert over denne returforbindelse (14) fra mottagningsstedet, først bevirkes ved konstatert manglende synkronisme av koder (4) og dekoder (8).

6. Overføringssystem som angitt i et av de foregående krav, k a r a k t e r i s e r t ved at der i klartekstapparatet (15) på sendesiden er anordnet en kobling (3) som i tidsavstander som kan tolereres for klarsignalene, eller i informasjonsfattige, fortrinns-vis informasjonsfrie, tidsavsnitt avgir til chifreringsapparatet (16) et styresignal (SynS) som i chifreringsapparatet (16) bevirker en innblending av innstillingssignalet i signalstrømmen (chifrert signal) fra sende- til mottagningsstedet.

Fig. 1

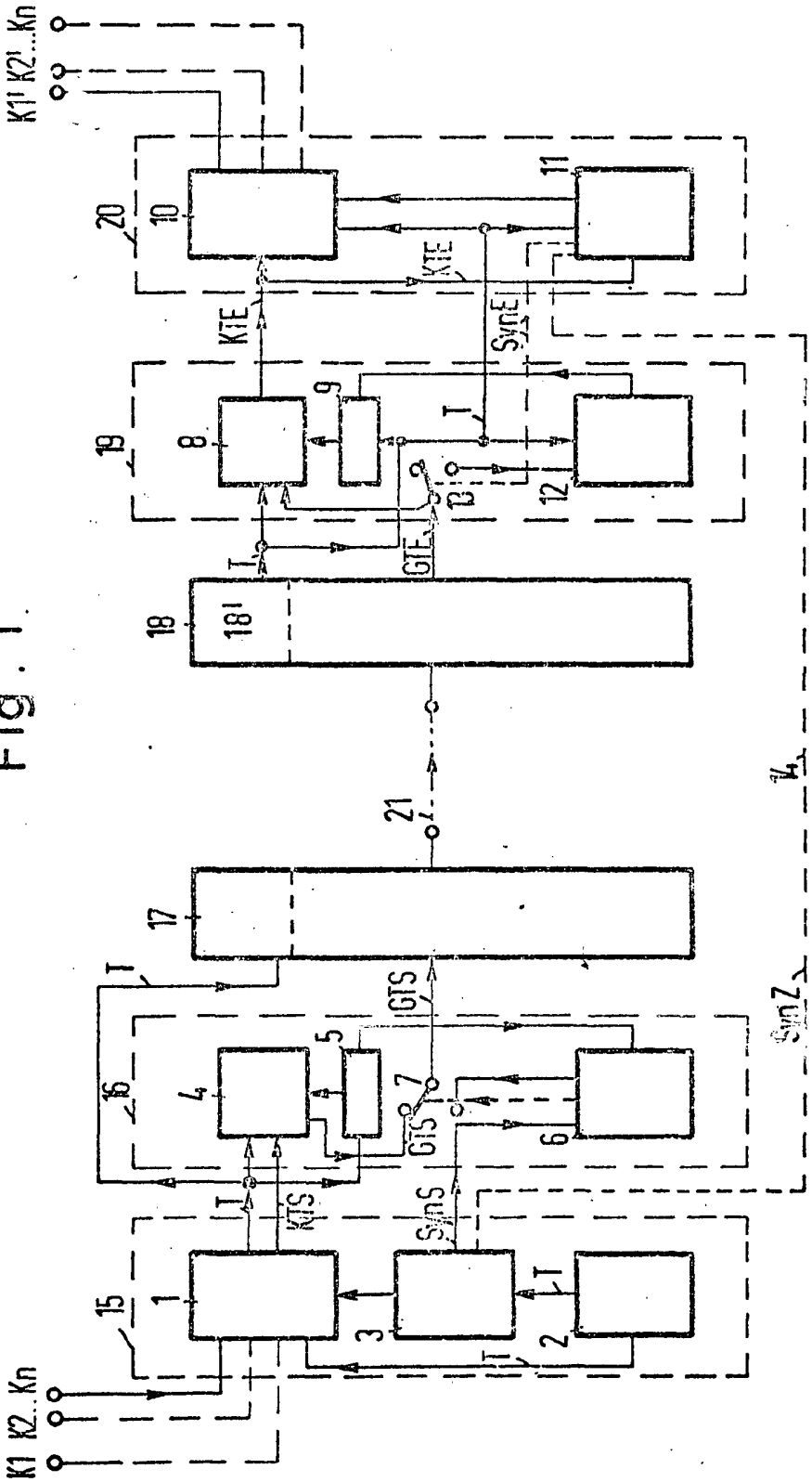
K1' K2'...Kn
K1 K2..Kn
KTE
SynE
GTE
GTS
SynS
SynZ
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
18'
19
20
21

Fig. 2