Acadm. Bibl.

compact

COMPUTER EN ACCOUNTANT

UIT DE INHOUD:

Klynveld Kraayenhof & co
ACCOUNTANTS

KMG
Klynveld Main Goerdeler
Accountants-international

NUMMER 25 8E JAARGANG HERFST 1981

COMPUTER EN ACCOUNTANT

INHOUDSOPGAVE

NUMMER 25 8E JAARGANG HERFST 1981

VAN DE REDACTIE

25 nummers van Compact is voorwaar geen kleinigheid.

Hoe het was: April 1974

"Voor u ligt het eerste nummer van Compact (Computer en accountant), een blad dat onder redactie zal staan van enkele leden van de Automatisering- en Controlegroep".
Een paar alinea's verder:
"De voornaamste doelstelling van Compact zal zijn bij deze "wedloop" (up to date blijven) de helpende hand te bieden en gerichte zo mogelijk compacte informatie te verstrekken omtrent de ontwikkelingen op het gebied van de automatisering en controle in binnen- en buitenland".
Oproep aan de lezers:
"Aarzel niet vragen te stellen, meningen te uiten, opmerkingen te maken omtrent alles wat u leest of gemist heeft. Dit is van groot belang, omdat er door allen nog veel geleerd kan worden".

Hoe is het geworden: Herfst 1981

"Voor u ligt het 25e nummer van Compact (nog steeds groen als het gras), een blad dat onder redactie is blijven staan van enkele leden van de Automatiserings- en Controlegroep, bijgestaan door rubrieksredacteuren en vele schrijvers. "Resultaat ruim 1.000 pagina's tekst"

Nabeschouwing over de doelstelling:
"Aan de voornaamste doelstelling wordt voldaan. Compacte informatieverstrekking: het zomernummer 1981 is even dik als no. 1 van april 1974; wel dubbelzijdig gedrukt gebiedt de eerlijkheid te vermelden. Onder invloed van de nieuwe ontwikkelingen op het vakgebied is het aantal van belang zijnde kennisgebieden toegenomen.
Dankzij veelzijdigheid van redacteuren en schrijvers vindt adequate bespreking plaats. Conclusie: Compact beantwoordt aan zijn doel".
Oproep aan de lezers:
"De schriftelijke reacties bleven uit? Of werden geïnteresseerde lezers de nieuwe schrijvers?"

Aan de totstandkoming van Compact hebben velen medewerking verleend. De redactie is u er erkentelijk voor.

Eén persoon echter willen wij gaarne in het volle zonlicht plaatsen:

mevrouw J.C. Grapendaal-Voordenhout

Zij heeft jarenlang onze breinweefsels leesbaar op papier gezet.
Van harte dank voor uw toewijding en vakkennis.

De inhoud van dit nummer bevat 2 hoofdartikelen: Kantoorautomatisering en Systeem 38. Beide artikelen zijn zeer up to date. De totstandkoming is geschiedt in teamverband. De als regel enige effectieve manier om Automatisering en Controle in kaart te brengen.

Met betrekking tot het artikel over Systeem 38 van IBM is te vermelden dat dit in dezelfde vorm is verschenen in het blad Monitor van IBM, dat door deze organisatie in veelvoud onder haar cliënten wordt verspreid. De heer Roos, schrijver van het artikel, ontving van IBM Nederland de opdracht om het produkt aan een beoordeling te ontwerpen, vooral gericht op de aspecten van interne controle. Hoewel het artikel een vrij technisch karakter heeft beveelt de redactie het ter lezing aan, daaraan gelijk de toezegging verbindend dat wij, gezien het belang van het S 38 voor de komende jaren hier in de volgende nummers op terug zullen komen.

U, lezer, wordt van harte uitgenodigd om uw bijdrage te geven ter aanvulling of commentaar. De redactie stelt gaarne plaatsruimte in Compact beschikbaar.

De Automatisering en Controle Groep wenst een ieder
fijne Kerstdagen en een Voorspoedig 1982.

Compact is een uitgave van de Automatisering en Controle Groep van Klynveld Kraayenhof & Co..

Het doel van deze uitgave is informatie te verstrekken over ontwikkelingen op het gebied van automatisering en controle in binnen- en buitenland.

Deze informatie is in de eerste plaats bestemd voor diegenen, die in de algemene controlepraktijk werkzaam zijn.

Redactie:
Drs. J.E. Huizenga,
A.W. Neisingh en
Prof. D. Steeman.

Kopij kunt U inleveren bij de secretaris van de redactie:
H.J.M. van der Wielen.
Adres:
Pr. Irenestraat 59,
1077 WV Amsterdam.
Postadres:
Postbus 7137
1007 JC Amsterdam.

AKTUALITEITEN

door A.W. Neisingh

Langverwachte wet op de privacy bij kamer ingediend

Minister De Ruiter: 'Niet voor 1985 van toepassing'

Waakzaamheid Persoonsregistratie:

'Wetsontwerp mist aansluiting op praktijksituatie'

Toch geheel onverwacht is onlangs het ontwerp van Wet op de Persoonsregistraties (privacywet) bij de Tweede Kamer der Staten Generaal ingediend.
Volgens ingewijden zal een wetsontwerp op de Centrale Personenadministratie (CPA) spoedig volgen.

Uit geluiden in de pers blijkt, dat het ontwerp privacywet niet op essentiële punten afwijkt van het voorstel dat reeds in het Eindrapport van de zgn. Commissie Koopmans (1976) was opgenomen.

Als essentialia van de privacywet noemen wij reeds:
* uitsluitend geautomatiseerde persoonsregistraties vallen onder de Wet;
* instelling van een Registratiekamer;
* registratieplicht van persoonsregistraties;
* recht op inzage en correctie;
* ook zich in het buitenland bevindende persoonsregistraties van in Nederland gevestigde houders vallen onder de Wet.

Wij zullen de ontwikkelingen blijven volgen en onze lezers informeren.

COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.

KANTOORAUTOMATISERING

door J. Balvert, A. van der Drift en drs. B.M. de Vries

1. INLEIDING

De ontwikkelingen op het gebied van de elektronica hebben geleid tot de aanbod van een breed scala van hulpmiddelen, die bij uitstek inzetbaar zijn voor het verrichten van kantoorwerkzaamheden. De inzet van deze hulpmiddelen op een al dan niet planmatige wijze heeft het fenomeen kantoorautomatisering opgeleverd. Kenmerkend voor kantoorautomatisering is de grote verscheidenheid van de hulpmiddelen of beter gezegd, van de ingrediënten van kantoorautomatisering.
Dit artikel poogt een resumé te geven van deze ingrediënten. De toepassing van meerdere ingrediënten geeft een toename van integratie middels automatisering te zien.
Op deze integratie en op de met kantoorautomatisering samenhangende problemen betreffende interne controle en beveiliging, zal in een volgend artikel worden ingegaan.
De nadruk in dit artikel ligt op de ingrediënten van de kantoorautomatisering en niet op de wijze waarop tot een planmatige ontwikkeling van kantoorautomatisering gekomen kan worden.

Het doel van het artikel is om de lezer kennis te laten maken met de vele vormen waarin kantoorautomatisering zich voordoet en ontwikkelt. Daarbij dient men zich te realiseren, dat vele van de in dit artikel genoemde ingrediënten aangeschaft kunnen worden voor prijzen, die ondanks de huidige economische recessie, voor veel middelgrote en zelfs kleine bedrijven "haalbaar" zijn. De ontwikkelingen van kantoorautomatisering en de daarbij optredende vormen van integratie, hetgeen consequenties heeft voor de mate van interne controle, laten zich derhalve moeilijk overzien.

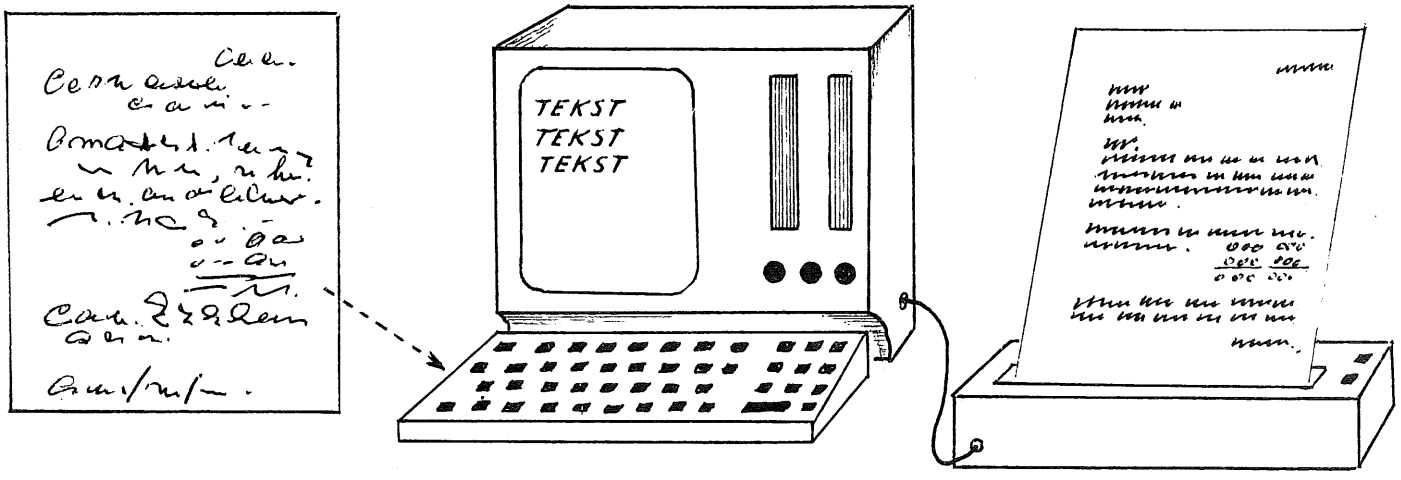
2. DE INGREDIENTEN VAN HET TOEKOMSTIGE KANTOOR

In dit hoofdstuk sommen wij de hulpmiddelen op die, naar de verwachting is, een rol zullen gaan spelen op het kantoor van de nabije toekomst. Zoals reeds in de inleiding is gezegd, letten wij daarbij niet op de mogelijkheden en complicaties die inhaerent kunnen zijn aan het benutten van die hulpmiddelen. Wij laten u slechts kennis maken met de ingrediënten van het toekomstige kantoor. Ter sprake komen:

2.1. Tekstverwerkende machine

De tekstverwerkende machine maakt het in hoge mate mogelijk met teksten te manipuleren en teksten van hoge kwaliteit af te leveren. De grote variëteit in de eigenschappen van deze machine en van het tekstverwerkende programma belet ons deze alle op te sommen. Wij beperken ons tot enkele hoofdzaken zoals het corrigeren en reviseren van teksten, het vasthouden van standaard-tekstdelen en afdrukkwaliteit.

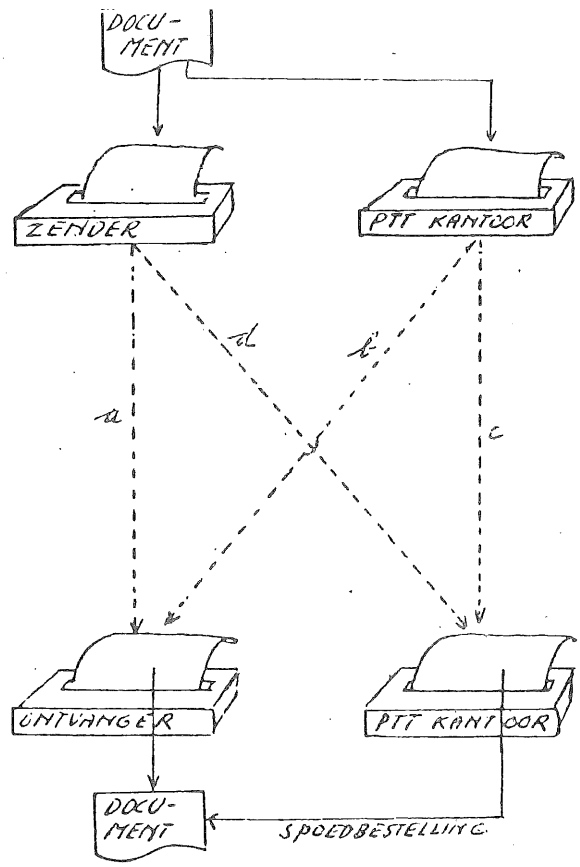
De tekstverwerkende machine kan een grote invloed hebben op de produktiviteit van de typist(e) en ook, doch veelal in mindere mate, op die van de samensteller van de teksten.



In opkomst is het via een telefoon of telegraaflijn koppelen van tekstverwerkende machines die op (grote) afstand van elkaar staan. Op deze manier kunnen teksten worden gedistribueerd.
Aan tekstverwerkende machines (wordprocessors) kan ook vaak een OCR-lezer gekoppeld worden. Met behulp van deze OCR-lezer kan een in concept getypte pagina van A4-formaat worden gelezen en naar de wordprocessor worden overgebracht ter correctie of nadere bewerking.

2.2. Facsimile apparatuur

Met behulp van een facsimile apparaat kan informatie, die is vastgelegd op een blad van A4-formaat, via een telefoonlijn worden overgeseind naar een ander facsimile apparaat, alwaar een identieke pagina ontstaat. Het bijzondere is, dat aan de wijze waarop de informatie op papier is vastgelegd nagenoeg geen eisen worden gesteld. Elk type letter alsook tekeningen, handtekeningen en foto's worden geaccepteerd. Het blad wordt in zijn geheel afgetast en overgeseind in een tijdsbestek van 1 tot 3 minuten. Er bestaat in navolging van de telefoongids een facsimilegids waarin alle bezitters van een facsimile apparaat worden genoemd. In ongeveer 200 postkantoren zijn ten dienste van het publiek facsimile apparaten opgesteld. Deze nieuwe vorm van dienstverlening door de PTT wordt TELEFAX genoemd. In onderstaande figuur zijn de mogelijkheden aangegeven.



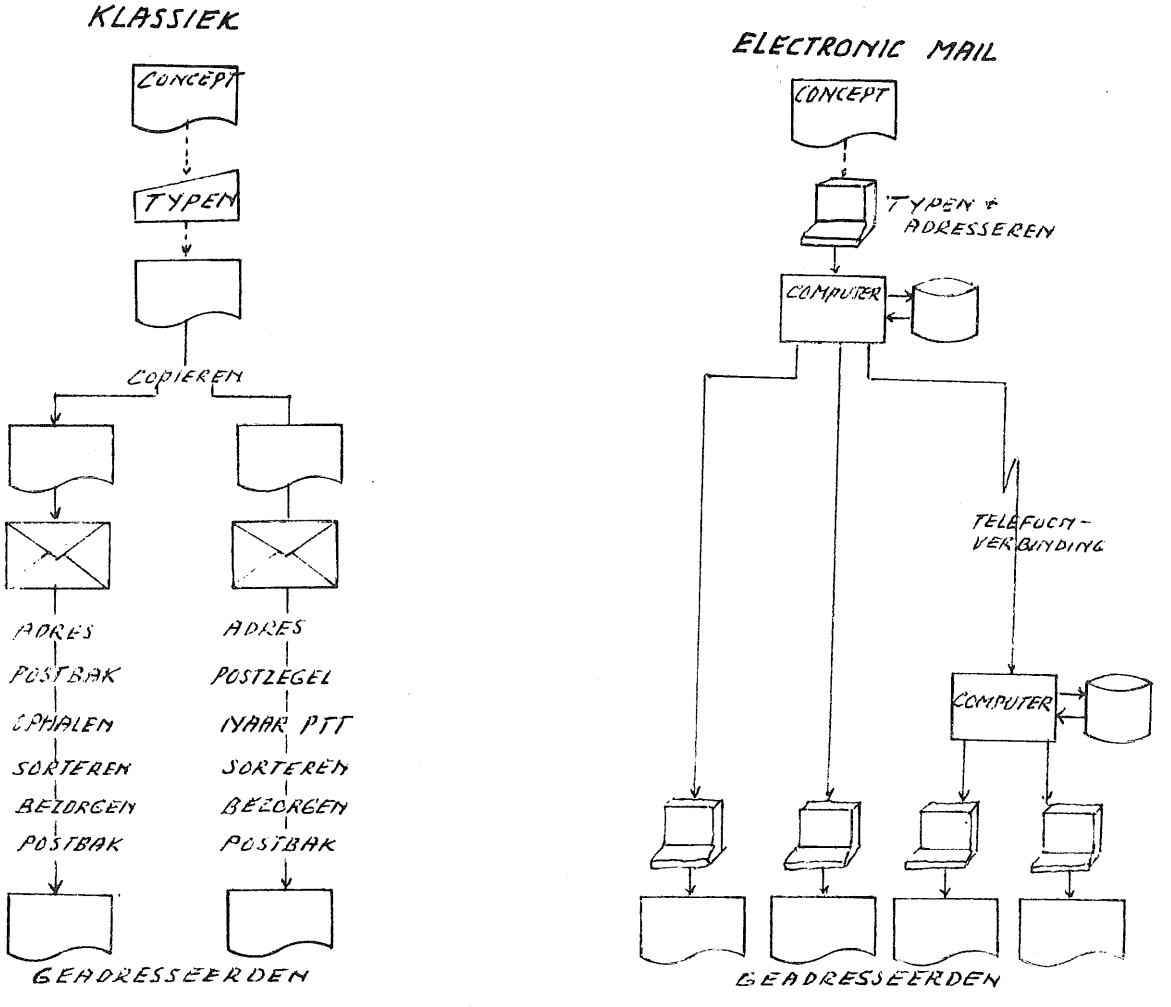
ad a: Zender en ontvanger komen beide in de facsimilegids voor.
ad b: Slechts de ontvanger heeft een facsimile apparaat.
ad c: Zender en ontvanger hebben beide geen facsimile apparaat.
ad d: Slechts de zender beschikt over een facsimile apparaat.

Het zal u inmiddels zijn opgevallen dat bij deze vorm van communicatie geen gebruik wordt gemaakt van een electronisch geheugen. De gegevens gaan rechtstreeks van papier naar papier.

In Chio (Verenigde Staten) zijn thans 3.000 abonnees die hun avondblad op deze wijze overgeseind krijgen.

2.3. Electronic mail (I)

Bezitters van een terminal (een beeldschermeenheid en/of een terminalprinter) kunnen berichten verzenden en/of ontvangen van andere terminalbezitters ongeacht de onderlinge afstand. Het principe van electronic mail (electronische postbezorging) is, dat een bericht naar een of meerdere gegadigden wordt verzonden en te bestemder plaatse op electronische wijze wordt gearchiveerd. De geadresseerde raadpleegt, op een moment dat hem dat uitkomt, zijn mailbox (brievenbus) en laat eventuele berichten op zijn beeldscherm verschijnen. Tenzij de geadresseerde het bericht laat afdrukken komt er bij deze wijze van berichtenuitwisseling geen papier aan te pas. Berichten komen op deze wijze binnen enkele minuten op hun bestemming. Daartegenover staat dat verzending via de PTT en/of via de interne postdienst enkele dagen kan duren.



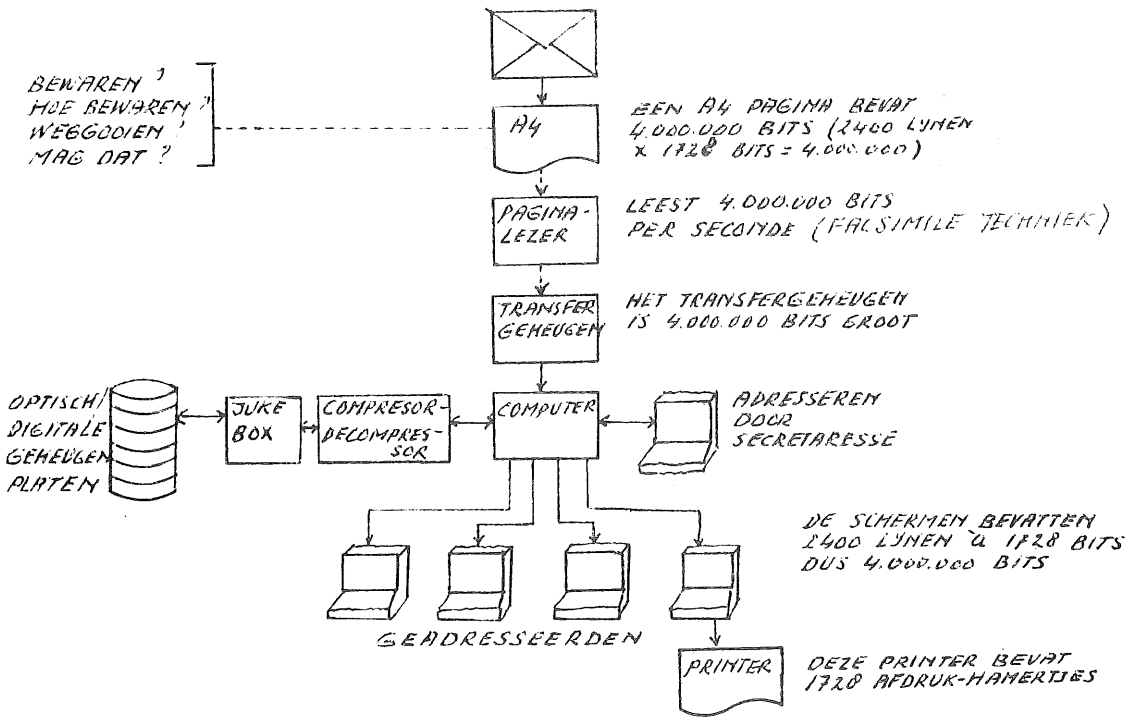
Electronic mail vereist de tussenkomst van een centrale computer met een "electronic mail" programma en een schijvengeheugen voor het opslaan van de post. Aan de vele funkties van een dergelijk programma gaan wij hier voorbij.

2.4. Electronic mail (II)

Bij de zojuist beschreven toepassing van electronic mail gaat het om berichten die allereerst met behulp van een toetsenbord zijn vastgelegd. Dit houdt belangrijke beperkingen in:

- Met de hand geschreven stukken moeten eerst worden getypt. Het is niet doenlijk externe stukken (fakturen, brieven, e.d.) over te typen.
- Handtekeningen, schema's, foto's en bijzondere tekens komen niet in aanmerking omdat slechts alfanumerieke gegevens met behulp van een toetsenbord naar een geheugen kunnen worden overgebracht.

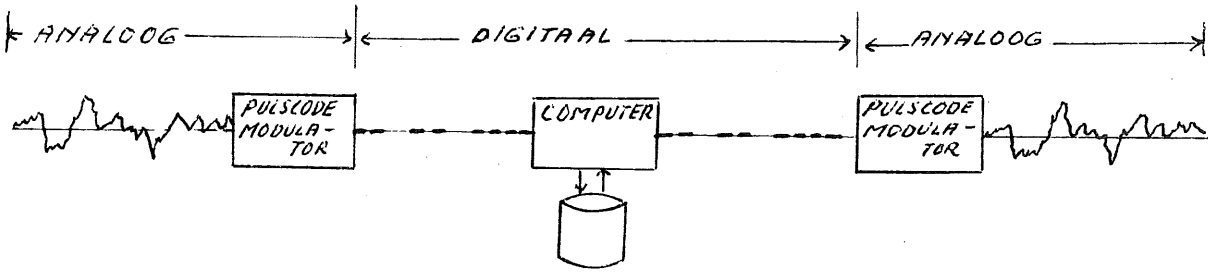
Deze beperkingen zijn op te heffen indien wij de te verspreiden documenten invoeren met behulp van de facsimile techniek en vervolgens opslaan in een geheugen dat dienst doet als mail-box. Dat geheugen zal bijzonder groot dienen te zijn want één A4 pagina bevat 4.000.000 bits.



Zo'n geheugen bestaat sinds kort. Het is een plaat waarin met behulp van laser 10.000.000.000 (10 miljard) bits kunnen worden ingebouwd. Aangezien bovendien de 4 miljoen bits van één pagina kunnen worden gecomprimeerd tot gemiddeld 400.000 bits (denk bijvoorbeeld aan het wit tussen teksten), kan één plaat 25.000 pagina's bevatten. Een juke box met 64 platen is dan goed voor 1,6 miljoen pagina's. Te veel van het goede ? Wellicht maar we moeten wel bedenken dat eenmaal ingebrande pagina's niet meer uitgewist kunnen worden om plaats te maken voor andere pagina's. Gearchiveerde pagina's kunnen worden opgeroepen door het intoetsen van een of meer trefwoorden die door de geadresseerde(n) zelf zijn aangebracht.

2.5. Digitalisering van spraak

Het gesproken woord plant zich op analoge wijze (als een "continu variërende kromme") voort via een telefoonlijn en leent zich daarom niet voor tussentijdse archivering. De spreker en de luisteraar staan altijd in direct kontakt met elkaar.
Sinds kort is men er in geslaagd om deze analoge informatie om te zetten in digitale informatie (bits). Ook het omgekeerde is mogelijk. Dit heeft vergaande consequenties want een computer kan bitreeksen analyseren en archiveren.

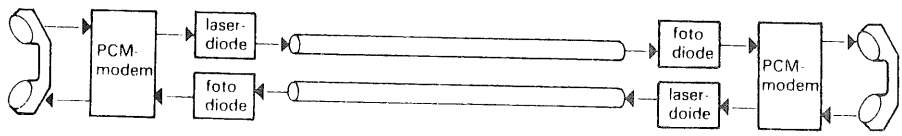


Wij sommen een aantal consequenties op:

a. Door analyse van bitreeksen kan de computer woorden herkennen. Het gaat hier om een kleine woordenschat die de betreffende spreker vooraf moet hebben ingesproken. Data-entry door middel van stemgeluid is dus in beperkte mate mogelijk. Vanzelfsprekend kunnen de ingesproken woorden ook worden afgedrukt.
b. De computer kan de mens toespreken. Ook hier is de woordenschat beperkt.
c. Het unieke stemgeluid van een spreker kan door de computer gecontroleerd worden op echtheid.
d. Een gesproken mededeling kan gearchiveerd worden in een mail-box en later door de bevoegde geadresseerde(n) worden afgeluisterd. Hij hoeft niet stand-by te zijn. Jammer dat de aldus ingesproken mededeling nog niet op papier kan worden afgedrukt.
e. Spraak kan over grote afstanden storingsvrij getransporteerd worden omdat beschadigde bits gerepareerd kunnen worden. Een vervormde analoge kromme kan niet hersteld worden.

2.6. De glasvezel

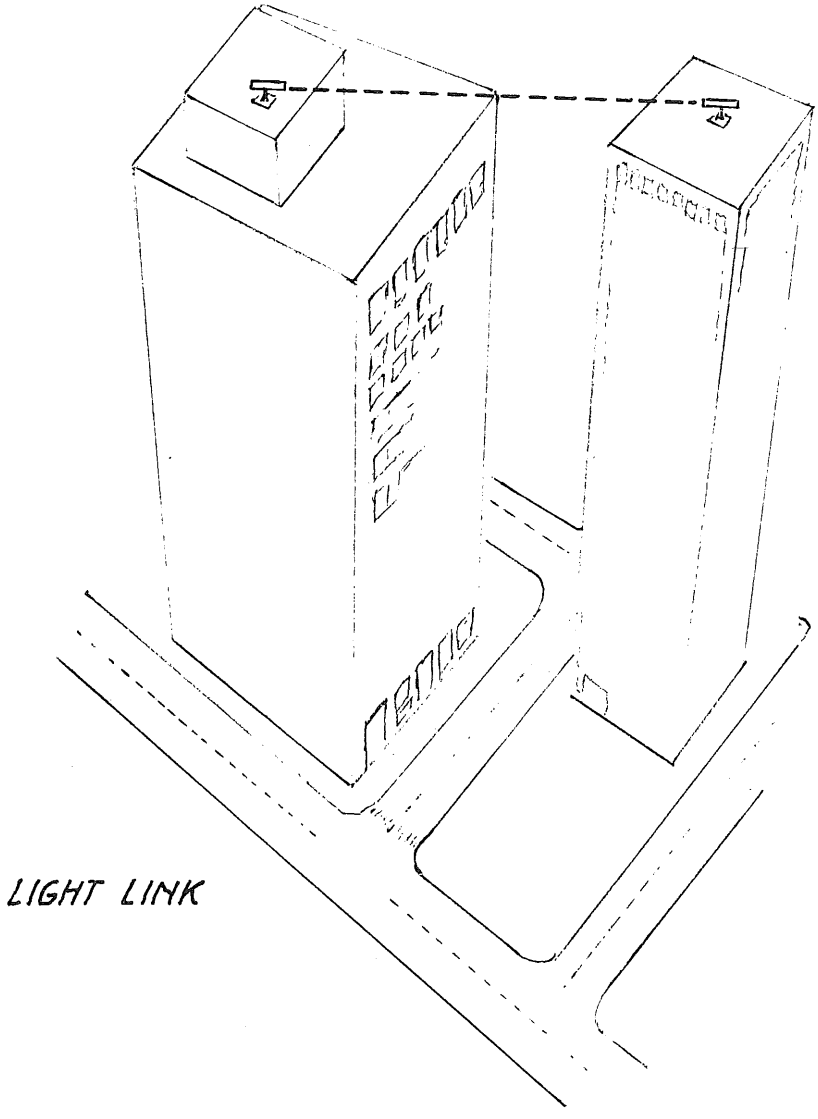
Het digitaliseren van de spraak heeft onder andere in Nederland een spectaculaire toepassing gevonden in een onderdeel van het telefoonnet gelegen tussen Helmond en Eindhoven. Tussen deze twee plaatsen is een ondergrondse glasvezelkabel gelegd met een zeer grote capaciteit. Uiteindelijk mikt men op 8.000 gesprekken over één twee-aderige glasvezelverbinding.



Ter vergelijking dient, dat in de 2-aderige koperen kabels tussen telefooncentrales 120 gesprekken op elkaar gestapeld kunnen worden. Een glasvezel is een van glas vervaardigde draad ter dikte van één tiende van een haar. Daardoor worden geen electrische impulsen gevoerd maar lichtimpulsen. Uit de tekening is af te leiden dat de analoge spraaksignalen allereerst worden gedigitaliseerd met behulp van een pulscode-modulator. De laser-diode zet vervolgens de electrische bits om in optische bits. Aan de andere zijde zorgt een foto-diode voor terugvertaling in electrische bits.
Een belangrijke eigenschap van een optische impuls is dat hij ongevoelig is voor inductie door naastgelegen kabels en dat hij zelf geen krachtenveld veroorzaakt. Hij kan dus storingsvrij werken en kan niet worden afgetapt. De digitalisering garandeert bovendien een onbeschadigd transport van de signalen. Gezien de grote investeringen in het PTT net is het niet de verwachting dat de dure koperen kabels op grote schaal zullen worden vervangen door de goedkope en efficiënte glasvezelkabels. Voor nieuwe toepassing in de sfeer van het toekomstige kantoor is dat wel het geval aangezien in de toekomst een veelheid van apparaten binnen het kantoor op efficiënte wijze en storingsvrij met elkaar verbonden zullen worden.

2.7. De Infraroodverbinding

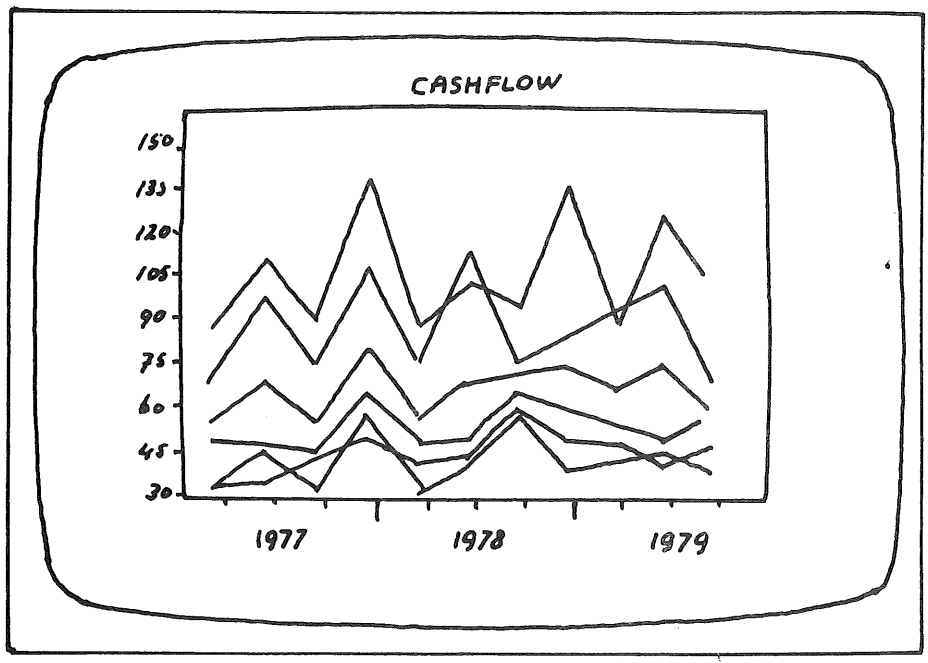
De infraroodverbinding is aan ieder, die weet hoe een televisietoestel op afstand wordt bediend, bekend. Het is een draadloze verbinding. De signalen bestaan uit impulsen van het onzichtbare infrarood licht. Daar waar kabelverbindingen onmogelijk zijn aan te leggen, bijvoorbeeld tussen twee op afstand staande kantoorgebouwen, is een light link een alternatief. Vanzelfsprekend wordt de glasvezel gebruikt voor de communicatie tussen de verdiepingen.



Draagbare zakterminals die infrarood licht uitzenden, kunnen diensten bewijzen aan hen die zich niet op een vaste plaats bevinden doch in het zicht van een infrarood ontvanger. Infrarood ontvangers bevestigd aan het plafond van een werkplaats of magazijn vergemakkelijken data-entry door monteurs, magazijnpersoneel en voorraadopnemers.

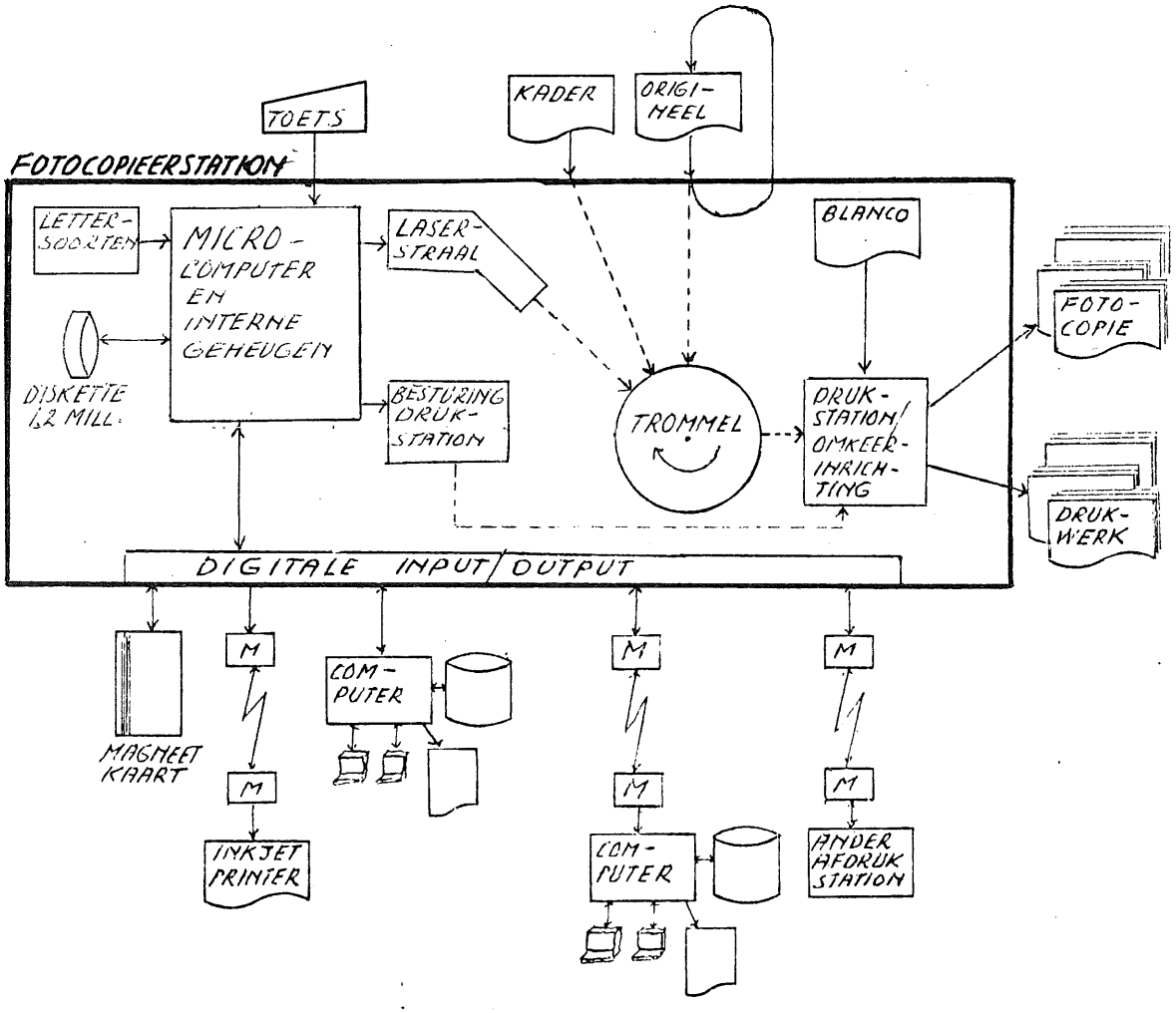
2.8. Grafiek en kleur

In toenemende mate is er belangstelling om gegevens die in computerbestanden zijn vastgelegd in de vorm van grafieken te presenteren in plaats van of ter aanvulling op computerlijsten. Er zijn programma's ontwikkeld die uit numerieke gegevens grafieken vervaardigen en daarin ook de gewenste kleurschakeringen kunnen aanbrengen. Vanzelfsprekend zijn er apparaten ontwikkeld om deze informatie aan de mens te presenteren. Er zijn beeldschermen op de markt die tot in zes kleuren toe grafieken voorzien van toelichtende tekst kunnen laten zien en printers om het geziene voor later vast te leggen.
Het kleurenbeeldscherm zal ook een bijzondere betekenis gaan krijgen bij het invoeren en opvragen van gegevens. Formulierindelingen en uitzonderingssituaties kunnen in kleur worden gepresenteerd.
Tenslotte is er het fotocopieerapparaat dat de kleuren van het origineel nagenoeg feilloos overbrengt naar de kopie.



2.9. Het fotocopieerstation

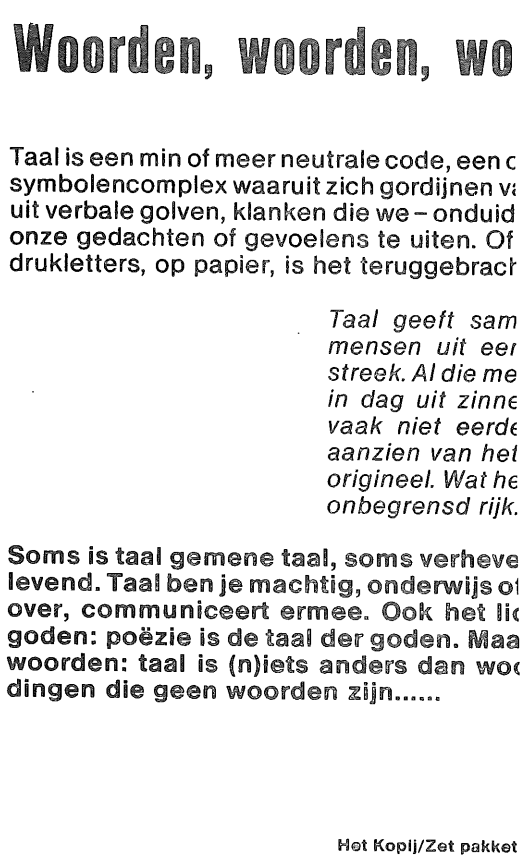
We hebben hier niet het gewone kopieerapparaat in gedachten maar een multipurpose fotocopieerapparaat, dat behalve de bekende funkties nog andere funkties heeft.
De input kan bestaan uit een pagina maar ook uit een reeks bits direct of via een telefoonlijn aangevoerd vanuit een computer. Het is tevens een printer en zo er geprint wordt volgens het ink-jet principe of het laserprincipe is er een keuze uit meerdere lettersoorten.
Tussen haakjes: Een ink-jet printer is een printer die per seconde tienduizenden kleine magnetisch geladen druppeltjes naar het papier spuit. Door ombuiging van de richting van de druppeltjes worden tekens gevormd.
Aan het origineel kan ook een kader worden toegevoegd met of zonder vaste teksten. Vanzelfsprekend produceert het apparaat het gewenste aantal kopieën en worden deze desgewenst gesorteerd afgelegd. Er kan dubbelzijdig gedrukt of gefotocopieerd worden.



Overigens rijst de vraag of de kopie wel altijd als een getrouwe weergave van het origineel is te beschouwen.

2.10. Fotozetapparaat

Een fotozetapparaat is een apparaat waarmee men met behulp van getypte teksten de layout van professioneel drukwerk kan geven.
Met het laatste bedoelen wij onder andere de mogelijkheid om te kiezen uit een grote bibliotheek van lettersoorten, groot of klein, vet of dun, cursief of rechtop, enzovoort. De tekst bestemd voor de fotozetter kan worden overgeseind vanuit een tekstverwerkende machine, op een diskette worden aangeleverd of ter plaatse worden ingetoetst. Ingetoetst worden ook de zetcodes die de gewenste layout besturen. Eventueel kunnen de zetcodes reeds met behulp van een tekstverwerkende machine tussen de tekst zijn geplaatst. De output van de fotozetter is een blad papier op A4-formaat, die men de foto noemt.



Woorden, woorden, wo

Taal is een min of meer neutrale code, een c
symbolencomplex waaruit zich gordijnen v
uit verbale golven, klanken die we – onduid
onze gedachten of gevoelens te uiten. Of
drukletters, op papier, is het teruggebrach

Taal geeft sam
mensen uit eer
streek. Al die me
in dag uit zinne
vaak niet eerde
aanzien van het
origineel. Wat he
onbegrensd rijk.

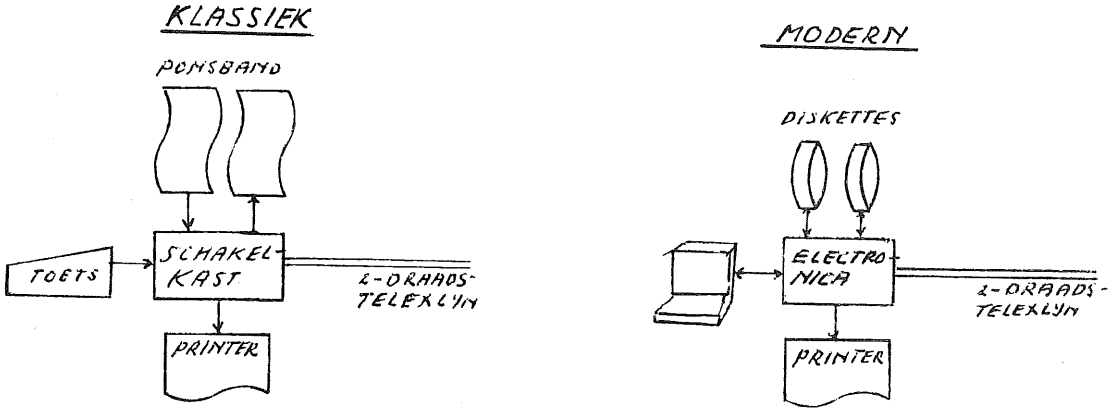
Soms is taal gemene taal, soms verheve
levend. Taal ben je machtig, onderwijs o
over, communiceert ermee. Ook het li
goden: poëzie is de taal der goden. Maa
woorden: taal is (n)iets anders dan wo
dingen die geen woorden zijn.....

Het Kopij/Zet pakket

Het meest opvallende aan de foto is het verzorgde uiterlijk.
Andere voordelen zijn de besparing op papierkosten en distributiekosten.

2.11. Telexapparatuur

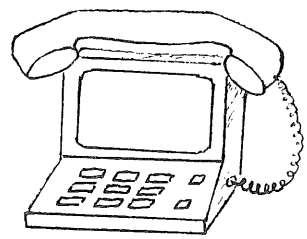
Telexen, ook telegraferen genoemd, doet men al vanaf 1882 toen een chef bij de Franse posterijen er in slaagde duidelijke internationaal geldende afspraken te formuleren. Zo op het eerste oog is men geneigd deze oude vorm van communicatie geen lang leven meer te geven. Dit is echter een onjuiste gedachte.
Door de sterke mate van standaardisering van de apparaten, de codes en het protocol omspant deze verbinding gemakkelijk de gehele aardbol en alleen in Nederland zijn er 30.000 telexaansluitingen.
Modernisering van de oude mechanisch werkende telexapparaten maakt dat het bestaan van de telex voor lange tijd gewaarborgd is.



Het moderne telexapparaat is in feite een kleine dedicated computer. Dit houdt in dat de funkties ook kunnen worden ondergebracht in een kleine of grote general purpose computer. Ook kan een tekstverwerkende computer voor telexdoeleinden geschikt gemaakt worden.
Indien daarbij verder bedacht wordt dat vele moderne computers onderling gekoppeld kunnen worden, dringt de gedachte aan integratiemogelijkheden zich op.

2.12. Het telefoontoestel

Bij het moderne telefoontoestel is de kiesschijf vervangen door kiestoetsen, hetgeen het maken van een verbinding aanmerkelijk versnelt. De PTT neemt proeven met een uitbreiding van haar dienstenpakket waarvan voornamelijk de particuliere gebruiker kan profiteren. Reeds nu is telefonisch vergaderingen voor groepen van 3 tot 22 deelnemers mogelijk na een voorafgaande afspraak. De komst van de videofoon, een telefoontoestel met een beeldscherm zal het vergaderen



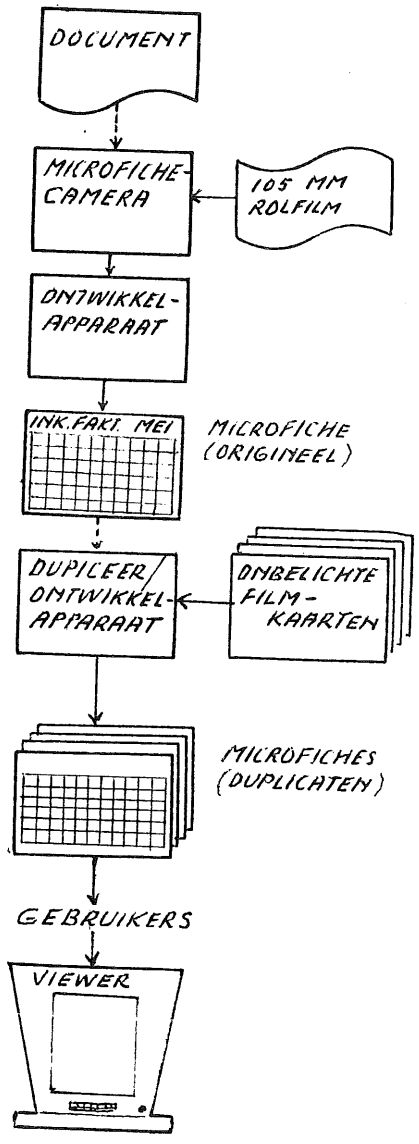
op afstand kunnen bevorderen. Het ligt ook in het verschiet dat het toetsenbord van het telefoontoestel als data-entry apparaat gebruikt zal worden.

2.13. Microfilm

Met behulp van een microfilmcamera kan een pagina worden vastgelegd op een filmbeeldje. Het oppervlak van dat filmbeeldje is (om een orde van grootte te noemen) 500 maal kleiner dan het oorspronkelijke document. Er zijn vele technieken bedacht om in een later stadium het betreffende document weer terug te vinden en zichtbaar te maken op het scherm van een viewer. Ook kan van het schermbeeld een hard-copy worden vervaardigd.
Bij de meest geavanceerde microfilmtoepassing wordt de administratie van de filmkartotheek bijgehouden door een computer. Een programma kan dan het gewenste document of de filmrol waarop het document is vastgelegd selecteren. Men noemt dit computer assisted retrieval.

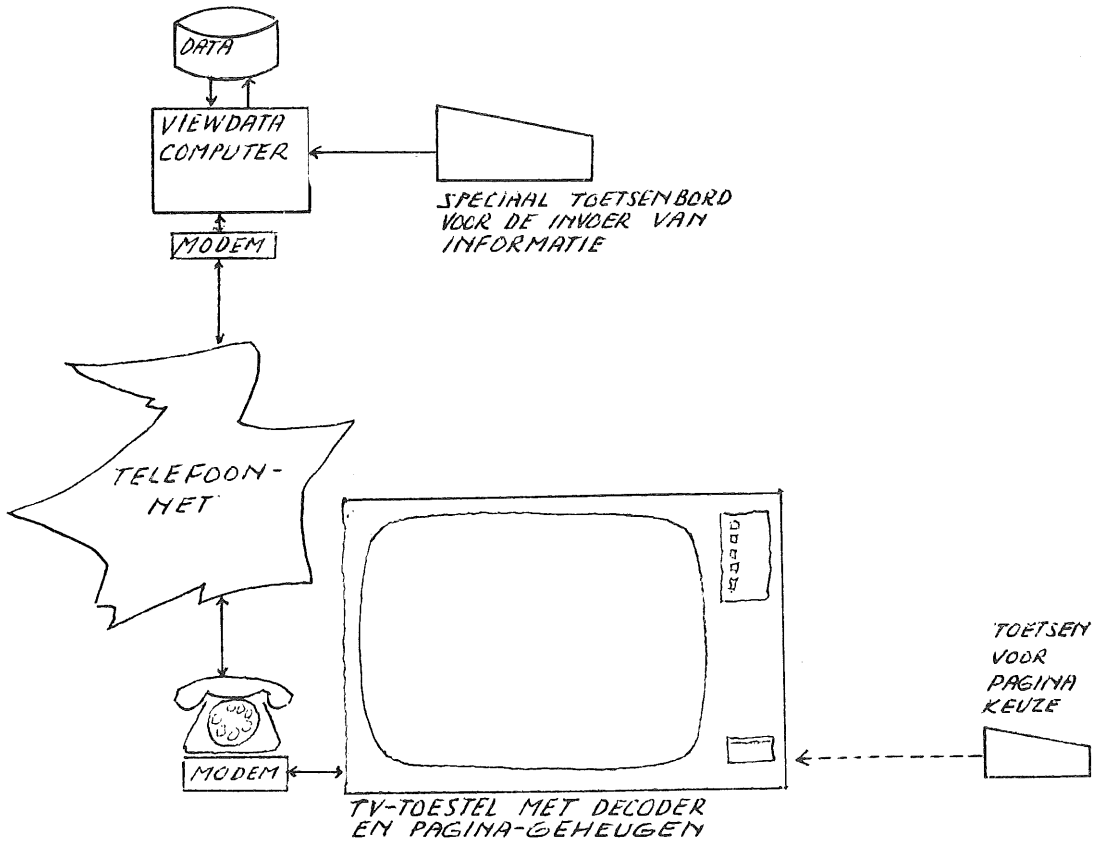
Vergelijken we het microfilmen met de electronic mail-methode genoemd onder 2.4. dan vallen in eerste instantie de volgende verschillen op:

a. Het terugzoeken van een electronisch gearchiveerde pagina gaat (mits men op de juiste trefwoorden mikt) beduidend sneller dan het terugzoeken van een filmbeeld.
b. De gevonden pagina wordt op het beeldscherm contrastrijker getoond dan op het scherm van de viewer.
c. De organisatie van de electronische kartotheek is vaak ingewikkelder dan van de microfilmkartotheek. Bij de laatste kan een handmatige indeling van de kartotheek in groepen een verlichting betekenen van het coderen van de filmbeelden.
d. Een electronisch vastgelegde pagina staat direct voor gebruik gereed van een niet van te voren vastgestelde groep gebruikers. Een filmbeeld komt pas ter beschikking nadat de filmrol vol is, ontwikkeld is en gedupliceerd is ten behoeve van met name genoemde abonnees.
e. Een electronische pagina wordt electronisch verzonden eventueel via de telefoonlijn. Een filmbeeld moet naar de gebruiker worden gebracht of per post worden verzonden.
f. De hier besproken electronic mailtoepassing vraagt een grotere investering dan de relatief goedkope microfilmmethode.



2.14. Viewdata

Het principe van viewdata, door de Nederlandse PTT viditel genoemd, zal u bekend zijn. De mogelijkheden die viewdata heeft voor de communicatie zijn nog niet geheel in kaart gebracht. Er is reeds een voor een ieder toegankelijke viewdatabank en er zijn viewdatabanken bestemd voor closed user groups. Het nut van deze databanken zal in sterke mate afhangen van de inhoud en van het up-to-date zijn daarvan.



Grote kantoren, vooral die met gespreide vestigingen, zouden een privé-databank kunnen benutten voor het snel verspreiden van berichten volgens het electronic mail principe. Een viewdata pagina kan de eigenaar(s) van die pagina verwijzen naar andere pagina's met voor hem (hen) bestemde berichten. De betreffende viewdata pagina fungeert aldus als mail-box.

2.15. Sensoren

De verdere ontwikkeling van op chips gebaseerde sensoren zullen de zintuigen worden van vele computerachtigen. Temperatuurverschillen, gewichtsverschillen, stemkarakteristieken, vingerafdrukken, lichtintensiteiten, kleurverschillen, hardheidsverschillen, afstanden, etcetera zullen door sensoren worden opgemerkt. De consequenties voor de besturing van apparaten zijn nog niet te overzien.

2.16. Microcomputers

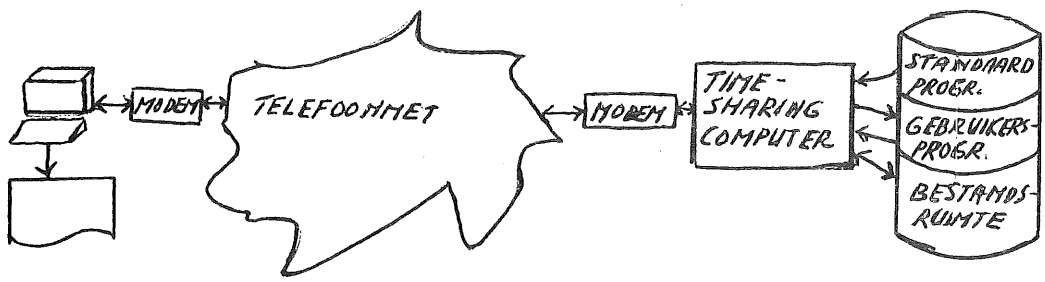
Microcomputers zullen blijkens de prognoses een grotere rol dan thans gaan spelen op het toekomstige kantoor. Op dit ogenblik zijn computers voornamelijk hulpmiddelen van die groep van medewerkers die een uitvoerende taak hebben. Zij worden gebruikt voor het voeren van voorraadadministraties en grootboekadministraties, het vervaardigen van statistieken, tekstverwerking, etc.. Het management maakt gebruik van de computeruitkomsten doch is wat zijn overige taken betreft nog pas in geringe mate in aanraking gekomen met de computer.
Het onderstaande overzicht, ontleend aan het boek "Het kantoor van de toekomst" van Willem Waterreus brengt het terrein in kaart waarop zich ergens de braakliggende plekken verschuilen die het doelwit zijn van de microcomputer.

	Top-management	Hoger management	Midden-management
1. Communicatie	38,3	26,8	19,5
2. Rekenen en plannen	7,0	11,3	12,5
3. Conceptvoorbereiding	15,7	19,8	18,2
4. Documentbehandeling	7,9	7,5	5,1
5. Opbergen en terugvinden	2,9	5,7	6,8
6. Informatie verzamelen	11,7	13,8	12,7
7. Kantoormachines gebruiken	0,2	1,9	11,3
8. Overige buiten kantoor	13,1	6,6	2,2
9. Rest	3,2	6,6	11,7
	100,0	100,0	100,0

Het zal onder andere van de vindingrijkheid van softwarehouses afhangen hoe snel en hoever de microcomputer in het management zal penetreren. Wellicht zullen zij hun aandacht richten op het met behulp van timesharing raadplegen van databanken (juridische-economische-financiële-) en het ontwerpen van planningsprogramma's en rekenmodellen.

2.17. Timesharing

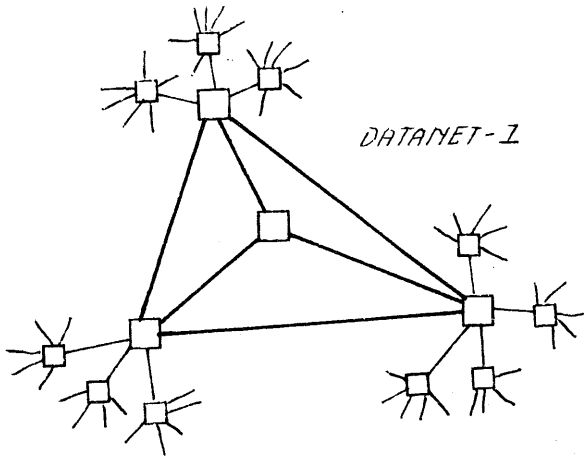
Timesharing betekent in wezen niet meer dan dat beschikbare computertijd verdeeld wordt tussen gebruikers die op een gegeven moment in verbinding staan met een computer. Meldt zich een nieuwe gebruiker of valt er een af, dan wordt de tijd herverdeeld.
In de praktijk echter heeft het begrip timesharing een ruimere betekenis gekregen. Het gaat daarbij om het via het telefoonnet ge-



bruik maken van de computer van een timesharing-centrum. In deze computer is een grote variëteit van programma's opgeslagen.
Het zijn standaardprogramma's zoals bijvoorbeeld financial forecasting, planning, sterkteberekening, wiskundige formules, etcetera.
De gebruiker kan ook zelf een programma ontwikkelen (Basic-taal) en dit invoeren in de timesharing-computer. Hij kan ook bestandsruimte reserveren. Wat de gebruiker nodig heeft is een geëigende microcomputer of terminal, een kies-modem en een gebruikersnummer.
Het is niet ondenkbaar dat kantoorpersoneel de timesharing-computer benut voor deel-administraties zonder dat dit aan de leiding van het kantoor bekend is.

2.18. Datanet-1

Datanet-1 is de naam van het eerste en enige openbare netwerk voor uitsluitend dataverkeer in Nederland. Het is opgezet en wordt beheerd door de PTT. Het is een deels maasvormig netwerk dat in totaal 61 knooppunten bevat waaronder een beheerscentrum in Bussum.



Het is de bedoeling dat Datanet-1 een belangrijke rol gaat spelen in het groeiend dataverkeer tussen terminals en computers en computers onderling. Het netwerk biedt enkele faciliteiten die niet ter beschikking staan als gebruik gemaakt wordt van telefoonnet.
Onder andere maakt het niet meer uit of de zender een andere transmissiesnelheid hanteert dan de ontvanger.
Het tarief is gebaseerd op de hoeveelheid door het netwerk getransporteerde gegevens en onafhankelijk van de tijdsduur van het gebruik.
Deze hoeveelheid wordt gemeten door het tellen van het aantal aan het netwerk toevertrouwde pakketten van een vast aantal bits en wel 1024 bits. De pakketten die tot één bericht behoren kunnen ieder een andere weg volgen door het netwerk en tijdelijk in knooppunten gebufferd worden (Packet switching). Voordat zij de eindbestemming bereiken worden de pakketten zonodig weer in de juiste volgorde geplaatst. Buffering houdt in dat een directe spraakverbinding onmogelijk is. Gesproken berichten bestemd voor een mail-box kunnen wel via datanet-1 verzonden worden.

SYSTEEM 38 BIEDT UITSTEKENDE MOGELIJKHEDEN VOOR REALISERING VEILIGE AUTOMATISERINGSORGANISATIE *

door H. Roos

De schrijver aan het werk met een Systeem 38.

De architectuur van het Systeem 38 wijkt zodanig af van de tot nu toe gebruikelijke computer-architectuur, dat er alle aanleiding is aandacht te besteden aan de invloed daarvan op beheersing en controleerbaarheid. Het is de bedoeling via dit artikel inzicht te verschaffen in de bijzondere eigenschappen van het Systeem 38 en de gebruiksmogelijkheden, die daardoor worden geboden. Het is niet de opzet alle faciliteiten volledig en uitputtend te beschrijven. Daarvoor wordt verwezen naar de officiële IBM publicaties. (1)

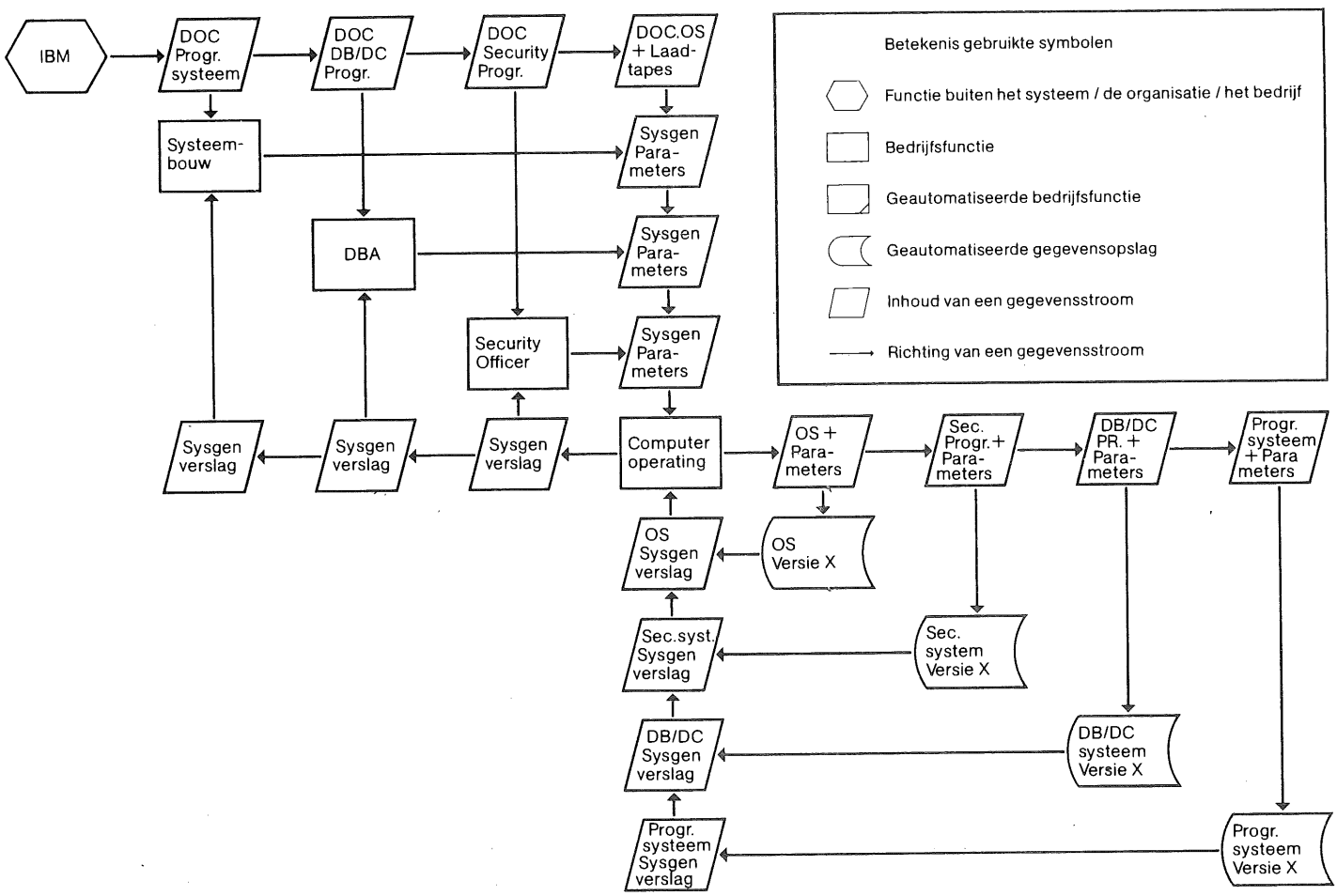
* De voor dit artikel gebruikte technische informatie over Systeem 38 en het CPF is ontleend aan de officiële IBM publicaties en aan de artikelen van Houden en Berstis, waarnaar is verwezen. De auteur kan er niet voor instaan dat de fysieke werking van het Systeem 38 en CPF steeds volledig daarmee in overeenstemming is.

Aangegeven wordt hoe een model automatiseringsorganisatie met Systeem 38 kan worden gerealiseerd. Om een goed inzicht te kunnen geven in de specifieke Systeem 38 architectuur wordt uitgegaan van een beknopte beschrijving van de traditionele computer-architectuur. In dit artikel wordt uiteraard ruime aandacht besteed aan de specifieke security-voordelen die de Systeem 38 "capability"-architectuur biedt en tevens aan de manier waarop deze via het CPF door de Systeem 38 gebruiker kunnen worden benut. Tenslotte geeft dit artikel de mogelijkheden en voordelen weer voor de controle-accountant.
De conclusie, die uit dit alles kan worden getrokken, is dat het Systeem 38 uitstekende mogelijkheden biedt voor het op een doelmatige wijze opzetten van een veilige automatiseringsorganisatie. Wanneer de accountant hiervan gebruik maakt kan hij er bij zijn controlewerkzaamheden zijn voordeel mee doen.

Beheersproblematiek

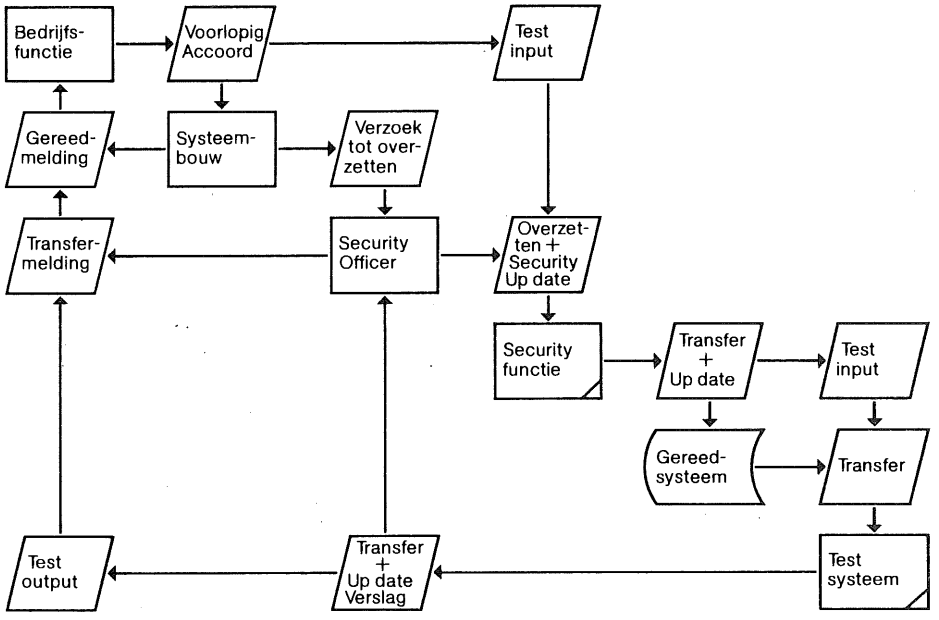
Het inschakelen van een computer in een bedrijf heeft tot gevolg dat de registraties van diverse bedrijfsfuncties centraal plaatsvinden. Zeker wanneer de computer gelijktijdig voor meer functies werkzaam is. Het is duidelijk dat dit een beheersprobleem oproept. Hieraan zit zowel een interne als externe kant. Met andere woorden, men moet het gebruik op doelmatige en doeltreffende wijze kunnen beheersen én het resultaat van het beheersen kunnen waarnemen.
Wil men een computersysteem beoordelen op zijn beheersingsmogelijkheden, dan zal men, gezien de verschillen in bedrijven en bedrijfsfuncties, dienen uit te gaan van een modelsituatie. In dit kader wordt hierna een model automatiseringsorganisatie als toetsingsraamwerk geschetst.
Het gebruik maken van automatisering als hulpmiddel in een bedrijf houdt in, dat er specialistische kennis nodig is, die echter relatief schaars is. Om van deze kennis nuttig gebruik te kunnen maken, zal zij moeten worden gebundeld in afzonderlijke bedrijfsfuncties. Op die manier ontstaat er een samenwerkingspatroon tussen bedrijfsfuncties in enge zin en de programmeurs- en operatorfunctie. Binnen dit samenwerkingspatroon, dat wordt gekenmerkt door delegatie, worden programma's geschreven, gecontroleerd en goedgekeurd volgens afgesproken procedures.
Indien systemen van verschillende bedrijfsfuncties identieke gegevens gebruiken, ligt een vorm van samenwerking voor de hand. De zich daarbij voordoende problematiek, betreffende de verdeling van de verantwoordelijkheid voor de juistheid en volledigheid van gemeenschappelijk gebruikte gegevens, voert naar een functie, die speciaal is belast met het coördineren en bewaken van goede afspraken hierover. Deze functie, de database-administratiefunctie, dient ervoor te zorgen, dat de tot stand gekomen afspraken correct in de systemen worden verwerkt. Tot de daarbij gehanteerde hulpmiddelen behoort de data

dictionary, een systeem voor het registreren van alle informatie over de gegevens en het gebruik ervan. Het up-to-date houden van de informatie daarin is niet eenvoudig. Vandaar dat het is aan te bevelen de database-administratiefunctie de bestandsdefinities te laten beheren.
Essentieel is dat de verschillende functionele scheidingen in het gemeenschappelijk gebruikte computersysteem worden gehandhaafd, namelijk die tussen operationele bedrijfsfuncties (de gebruikers), de systeembouwfuncties en de gegevensbeheersfunctie in de persoon van de database-administrator. Geen van de functies domineert de beide andere.
Voor het beheer van deze scheiding is een vierde functie nodig, namelijk die van security officer, onder wiens verantwoordelijkheid systemen tussen de verschillende afgebakende terreinen (contexten) kunnen verhuizen. De wijze waarop de scheiding tussen de contexten en de contexten zelf tot stand komen, is weergegeven in figuur 1.



Figuur 1. Een schema van de creatie van de primaire machine- en systeemcontext.

Essentieel voor het accepteren van nieuwe of gewijzigde systemen is dat de gebruikers zich van de kwaliteit van het systeem kunnen overtuigen. In deze zogeheten acceptatietestfase mag de systeembouwfunctie op eigen gezag geen wijzigingen meer aanbrengen. De operationele bedrijfsfuncties (produktiecontexten) kunnen voor dit testen niet worden gebruikt ter bescherming van de daar aanwezige actuele bedrijfsinformatie. Vandaar dat er een acceptatiecontext nodig is.
De overgang van systeembouw naar testfase is weergegeven in figuur 2.



Figuur 2. Een schema van de overgang van de systeembouwfase naar de testfase.

Gemeenschappelijk systeemgebruik

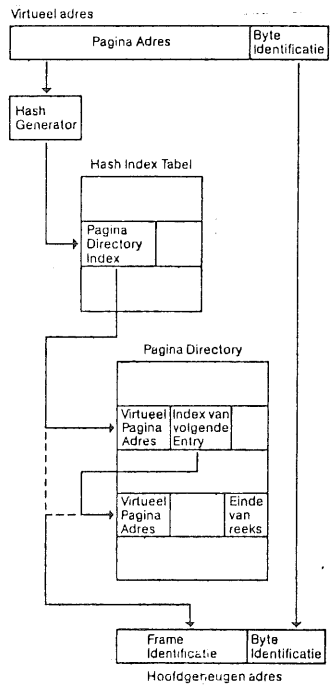
Zoals uit het voorgaande duidelijk is geworden, bevinden de gegevens van verschillende bedrijfsfuncties zich in dezelfde machine.
Wanneer er sprake is van multiprogrammering zullen bovendien tegelijkertijd verschillende processen bestaan. Tegelijkertijd zullen gegevens van verschillende registratieve systemen worden bewerkt en in- en uitgevoerd met behulp van verschillende of dezelfde programma's.
In een dergelijke situatie mogen programma's elkaar en elkaars gegevens niet ongecontroleerd beïnvloeden.

Uiteraard concentreert zich alles op het gemeenschappelijk geheugengebruik (2). Om te voorkomen dat gegevens en programma's elkaar daar gaan beïnvloeden, is het nodig geheugenbescherming toe te passen.

Dit gebeurt in principe door elk proces een sleutel toe te kennen, die moet passen op het slot van de bij dat proces behorende geheugenruimte.
Het toekennen van sleutels en het aanbrengen van de sloten dient te gebeuren door een overkoepelend proces, ofwel de systeemprogrammatuur. Alleen deze besturingsprogrammatuur mag de daarvoor benodigde instructies gebruiken.
De machine moet in een bepaalde status verkeren, de zogeheten privileged state, om deze instructies te kunnen gebruiken. Het toekennen van deze status aan een proces vindt plaats doordat de hardware als gevolg van een interrupt het besturingsprogramma tot het actieve proces maakt. In dat geval is het gehele geheugen toegankelijk. Het spreekt vanzelf dat dit alleen goed kan werken, als het besturingsprogramma betrouwbaar is en geen fouten bevat.
Een tweede mogelijkheid om de processen ten opzichte van elkaar af te schermen is gebruik te maken van capabilities, of wel door de machine toegekende unieke namen voor programma's, bestanden, enzovoorts (3). Als gevolg hiervan kan het bestand of het programma in beginsel alleen worden gebruikt door de maker ervan. Deze kan echter de machine instrueren ook anderen met deze naam toe te rusten, waardoor de bevoegdheid ontstaat om met die programma's en bestanden te werken. Uiteraard is dit alleen zinvol, als men de unieke naam niet kan wijzigen.
Deze unieke naam of pointer wordt door de machine in beschermd geheugen opgeslagen. Elke poging om die informatie te veranderen leidt automatisch tot vernietiging van de pointer. Dit principe nu wordt in het Systeem 38 toegepast.

Systeem 38 architectuur

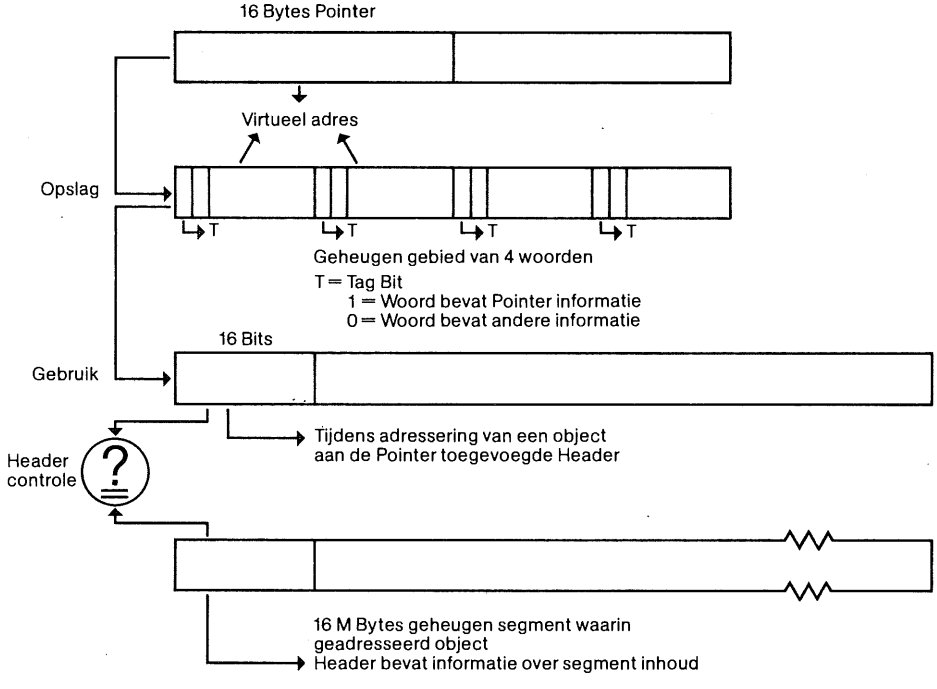
Het Systeem 38 wijkt door twee eigenschappen af van de "privileged state" architectuur. Er wordt geen onderscheid gemaakt tussen intern en extern geheugen; de programmeur heeft één groot lineair geheugen voor programma's en bestanden. Hierdoor is er geen zichtbare relocatie nodig van objectprogramma's. In de tweede plaats ondersteunt de machine zowel de primitieve "scalar" gegevenstypen (het adresseren van geheugenwoorden) als objecttypen (het adresseren van gegevensverzamelingen van verschillende typen).
De programmeur kan werken met een adresruimte van 2^{48} bytes, of wel 16 miljoen adresruimten van elk 16 miljoen bytes.



Figuur 3. Een schematische weergave van de hash-methode, waarvan ook het Systeem 38 gebruik maakt.

Deze omvang is nodig om vrijwel onbeperkt met unieke adressen te kunnen werken (4). Het vertalen van een dergelijk omvangrijk virtueel adres van 48 bits kan niet meer efficient via tabellen geschieden. Vandaar dat het Systeem 38 gebruik maakt van een hash-methode, zoals in figuur 3.

Het virtueel geheugen is verdeeld in segmenten van elk 16 M. Per segment wordt één object-type opgeslagen. Elk segment heeft een voorvoegsel van 16 bits, waarin de kenmerken van de in het segment opgeslagen objecten staan. Hiermee wordt gecontroleerd of de bewerking van een bepaalde instructie mogelijk is. Daartoe voegt de machine aan de pointer 16 bits toe met informatie over de eigenschappen, waaraan het geadresseerde object volgens de uit te voeren instructie zou moeten voldoen. Als het aldus bepaalde 16 bits patroon niet gelijk is aan het voorvoegsel (header) van het geadresseerde 16 M segment, wordt de instructie niet uitgevoerd. Zie figuur 4. Een tweede vorm van bescherming wordt geboden door elk woord van 32 bits uit te breiden met 8 extra bits. Een daarvan bevat een zogenaamd "tag"-bit, met behulp waarvan pointer-informatie wordt beschermd. Zie eveneens figuur 4.



Figuur 4. Een overzicht van de pointerbescherming met tagbits en de objectbescherming met headers of voorvoegsels.

Voordat een object kan worden geadresseerd, moet de systeem-pointer naar dat object worden uitgerekend, waarvoor een "resolve system pointer instruction" wordt gebruikt.
Deze instructie zoekt het object met behulp van zijn symbolische naam in operand 2 op. Daarbij wordt eventueel gebruik gemaakt van de systeem-pointer in operand 3, die verwijst naar de daarbij te gebruiken bibliotheek. Het resultaat is dat de "adresseerbaarheid" van het object wordt opgeslagen in de systeem-pointer in operand 1. Systeem-pointer-informatie wordt altijd in het "tagged" geheugen opgenomen. Alle andere gegevens worden opgenomen in geheugens waarvan de tag-bits op nul zijn gezet. Bij het uitvoeren van andere dan systeem-pointer-instructies worden alle tag-bits van dat geheugen op nul gezet en wordt de pointer vernietigd (5).

De object-typen die het Systeem 38 kent, zijn zogenaamde gestructureerde gegevenstypen, die in beginsel worden gedefinieerd door de verwerkingen die erop kunnen worden uitgevoerd. Een systeem-pointer bijvoorbeeld kan alleen worden gebruikt als doel(target)-operand in een beperkt aantal pointer-manipulatie-instructies.
Men onderscheidt twee groepen object-typen, namelijk systeemobjecten en programma-objecten. Systeemobjecten zijn onder meer data space, process control space, gebruikersprofiel en programma.
Programma-objecten zijn onder meer data-objecten, instruction definition list, operand list en exception description. Hierbij dient met nadruk te worden gesteld, dat een proces geen object is.
Een object bestaat uit een functioneel deel met de definitie van het object, en uit een zogenaamd "space"-deel, waarin de gegevens staan, die voldoen aan die definitie. Adressering van een object gebeurt door een systeem-pointer, adressering van een woord binnen de bijbehorende space door een space pointer.
Om een programma te kunnen creëren moeten eerst de noodzakelijke programma-objecten worden samengesteld. De "create program" instructie gebruikt als operanden de object definition tabel (ODT) en de instructions stream. De ODT geeft van elk programma-object het type en de functionele locatie, of wel naam, van het object. Het gecreëerde programma bestaat uit een functiedefinitie en een space deel met instructies. De instructie-operanden refereren aan de objecten uit de ODT.
Elk programma-object wordt gecreëerd op dezelfde manier als een programma.
De "create object" instructie voor het specifieke object-type bevat naast de operator een of meer operanden, waarbij de eerste de systeem-pointer is om de adressering mogelijk te maken en de volgende de definitie van het te creëren object.

Bij elke "create" instructie kan worden opgegeven in welke bibliotheek het te creëren object moet worden geplaatst. Daar de bibliotheek ook een object is, moet die dan eerst zelf zijn gecreëerd. Een bibliotheek bevat de relatie tussen de symbolische identificatie van

een object en het virtueel adres van dat object. In een programma bevat de ODT de symbolische identificatie. Via de bibliotheekinformatie kan worden vastgesteld of een object bestaat en of de gebruiker voldoende bevoegd is.
Er zijn twee soorten bibliotheken, namelijk de machinebibliotheek die door de machine wordt gecreëerd en de door de gebruiker gedefinieerde bibliotheken. Een gebruiker kan geen systeem-pointer krijgen naar de machinebibliotheek. Deze laatste bevat de adresseerbaarheid naar bibliotheken en naar gebruikersprofielen.
Uitvoering van een instructiereeks gebeurt in de vorm van een proces, dat eerst via een process control space moet worden gecreëerd. Daarna moet een "initiate process" instructie worden uitgevoerd. Om een primair proces te creëren en te initialiseren is een speciale machinefunctie beschikbaar.
Deze initial micro program load (IMPL)-functie creëert impliciet als laatste stap een proces, waarmee een initieel programma kan worden geladen.
De brongegevens moeten bestaan uit definities van bepaalde objecten. Dit zijn een gebruikersprofieldefinitie, een programmadefinitie en een procesdefinitie.
Het primaire gebruikersprofiel dat wordt gecreëerd is het eerste en dus eigenaar van zichzelf.
Het programma dat wordt gedefinieerd gaat lopen als het initiële proces is voltooid.
Omdat er nog geen objecten zijn, waaraan in de programmadefinitie kan worden gerefereerd, kunnen daarin geen objectverwijzingen worden opgenomen. De machine verwijst zelf naar het gecreëerde gebruikersprofiel en naar het gecreëerde programma.
Om alle machinefuncties te kunnen gebruiken zal het eerste gebruikersprofiel volledige bevoegdheid moeten bevatten.

Op basis van het eerste proces en het eerste gebruikersprofiel kan een volledig systeem van toepassingen worden gebouwd. Het daarbij behorende security-systeem kent twee groepen van bevoegdheden, die haaks op elkaar staan, namelijk systeem- en objectbevoegdheden.
Systeembevoegdheden betreffen het gebruik van objecten in algemene zin.
Objectbevoegdheden betreffen de bevoegdheid om van een bepaald object gebruik te maken.
Als men van het systeem gebruik wil maken, moet men er bekend zijn.
De eerste gebruiker kan nieuwe gebruikers toelaten door voor ieder een profiel te creëren en in de profieldefinitie op te geven welke systeembevoegdheden die gebruiker heeft.
Passwords kunnen niet in het gebruikersprofiel worden opgenomen. Op machine-niveau is elke gebruiker bekend door zijn identificatie.
De eerste gebruiker kan profielen voor een ander creëren. Hij behoudt als eigenaar alle bevoegdheden over de profielen. Bovendien worden alle bevoegdheden, die door anderen aan dat gebruikersprofiel worden toegekend ook impliciet aan hem toegekend (all object bevoegdheid).

Als een gebruiker tot het systeem is toegelaten, heeft hij automatisch alle bevoegdheden om alle objecten, buiten die waarvoor privileged instructions nodig zijn, te creëren. Hij kan deze ook aan anderen verlenen door middel van een "grant object authority" instructie. Daarin kan een specifiek gebruikersprofiel als target operand worden aangegeven. Wordt daarvoor nul gebruikt, dan gelden de in de derde operand gespecificeerde bevoegdheden voor alle gebruikers waarvoor een gebruikersprofiel bestaat. In dat geval spreekt men van public bevoegdheid.
De verschillende bevoegdheden die kunnen worden gespecificeerd zijn: object control, object management, authorized pointer, space authority, retrieve, insert, delete en update. De laatste vijf heten gezamenlijk operationele bevoegdheden.
Public objectbevoegdheden worden opgenomen in het functionele deel van het desbetreffende object. Persoonlijke objectbevoegdheden worden opgenomen in het gespecificeerde gebruikersprofiel.

Bij het creëren van een programma kan worden opgegeven dat het moet lopen onder het profiel van de eigenaar naast dat van de gebruiker. Tevens kan worden aangegeven of dit eigenaarsprofiel ook geldt voor programma's die door het onderhavige programma worden aangeroepen.
Ook bij proceswisselingen die samenhangen met multiprogrammering functioneert Systeem 38 op een unieke wijze. De machine kent per proces drie zogenaamde interne fasen, namelijk initialisatie, verwerking en beëindiging. Een proces in een verwerkingsfase kan actief zijn of opgehouden. In actieve staat kan een proces lopen of gereed zijn. Een proces wordt opgehouden als het wacht op een gebeurtenis of als het de beschikbaar gestelde tijd heeft opgemaakt. Het aantal tegelijkertijd actieve processen kan worden beperkt.
De wisseling van processen in de interne fasen gebeurt op microprogrammaniveau. Er zijn geen machine-instructies die dit direct besturen. Er kan richting aan worden gegeven door het "event" en "exception" management.
Exceptions zijn in het Systeem 38 signalen, die worden veroorzaakt door het eigen proces of signalen die de gehele machine betreffen. Events zijn gebeurtenissen die wel zijn voorzien, maar waarvan niet bekend is wanneer ze optreden. Zij dienen voor de synchronisatie van samenwerkende a-synchrone processen.
Het grote verschil ten opzichte van een "privileged state interrupt driven" machine-architectuur is dat het Systeem 38 een single task machine is. Binnen elk afzonderlijk proces kan worden bepaald op welke manier er op een signaal van een ander proces zal worden gereageerd. Dit kan variëren van negeren tot beëindigen van het proces. Daartoe moeten "exception" definities worden opgenomen in elk programma. Voor elk event of klasse van events moet binnen het proces of de proceshiërarchie een event monitor zijn geactiveerd, die de informatie bevat over de wijze van afhandeling van een event.

Control Program Facility

Het aantal keuzemogelijkheden, dat de machine-interface biedt, is bij het Systeem 38 zo omvangrijk, dat het voor een computergebruiker uiterst moeilijk is te hanteren. Vandaar dat het Systeem 38 is voorzien van een verzameling objecten onder de naam Control Program Facility (CPF) en van een aantal programmageneratoren, zoals een Source Entry Utility, een Data File Utility en RPG III.
Voorts is een COBOL compiler beschikbaar.
CPF bestaat uit een "Control Language" en een "Data Description Specification" faciliteit. De control language bevat een groot aantal commando's, waarmee objecten kunnen worden gecreëerd en beheerd, toepassingsprogramma's kunnen worden opgeroepen en beheerd, en het werk op het systeem, de verschillende systeemfuncties en componenten kunnen worden beheerd. Bij CPF horen ook standaardobjecten en een basis security systeem. De combinatie van commando's, standaardobjecten en basis security is voldoende om het systeem snel operationeel te maken voor de systeembouwfunctie en de database administratie-functie. Alle Systemen 38 hebben dezelfde gebruikers interface, omdat CPF alleen in zijn geheel kan worden geladen.

Commando's zijn in feite programma's en dus systeemobjecten.
Daarom kan ook voor elk programma worden bepaald welke objectbevoegdheden ervoor gelden. Alle commando's zijn public, behalve de commando's die gebruik maken van security machine-instructies. Bij het laden van CPF worden de volgende standaard gebruikersprofielen gecreëerd: security officer, programmer, work station user, system operator, programming service representative en customer engineer.
De eerste en beide laatste profielen kunnen in beginsel niet worden gewijzigd of verwijderd.
Naar behoefte kunnen andere gebruikersprofielen worden gecreëerd voor individuele gebruikers of voor groepen. Een dergelijk profiel bevat een gebruikersidentificatie, een lijst van objecten waarvan hij eigenaar is, een lijst van andere objecten waarvoor hij bevoegdheden bezit en een lijst van gebruikers die bevoegdheden hebben op zijn objecten. Daarbij is ook de aard van de bevoegdheden aangegeven.
Ten opzichte van het machine-interface bevat CPF extra mogelijkheden. De belangrijkste zijn de mogelijkheden om een gebruikerspassword en een initial program vast te leggen. Met behulp van het password gaat het systeem de betrouwbaarheid van de identificatie na en selecteert het juiste gebruikersprofiel. Daarna wordt als eerste programma het in zijn profiel gespecificeerd initial program geactiveerd. Op die manier kan efficiënt en doeltreffend gebruik worden gemaakt van menu security.
Bij de standaardprofielen behoren standaard-passwords. Een van de eerste activiteiten van de security officer zal dan ook zijn het wijzigen van zijn standaard-password SECOFR in een alleen aan hem bekend woord. Ditzelfde zal hij doen voor de programming service representative en de customer engineer. Hij behoudt zo de controle over het gebruik van die profielen.

Voor de gebruikers is het security-systeem hiërarchisch opgebouwd. De security officer staat aan de top. Alleen hij kan nieuwe gebruikersprofielen creëren en bestaande wijzigen of verwijderen. Alleen hij kan de passwords zichtbaar maken. Ook beschikt hij alleen over "all object" bevoegdheid.
Het CPF security-systeem kent evenals de machine-interface zogenaamde speciale bevoegdheden en objectbevoegdheid. De speciale bevoegdheid kent twee mogelijkheden, namelijk "save system" bevoegdheid en "job control" bevoegdheid.
De objectbevoegdheid omvat objectbevoegdheid in engere zin en gegevensbevoegdheid. Er zijn drie soorten objectbevoegdheid, namelijk in de eerste plaats om objecten te vernietigen of het eigendom ervan over te dragen, in de tweede plaats om een object naar een andere bibliotheek over te brengen en andere gebruikersbevoegdheden te verlenen of te ontnemen en in de derde plaats het gebruiksrecht. Dit laatste omvat in een aantal gevallen ook bepaalde gegevensbevoegdheden, afhankelijk van het type object.
Voor het object-type-bestand omvat het gebruiksrecht geen gegevensbevoegdheden. Voor een bibliotheek is er alleen het recht om te lezen en voor een programma het recht op toevoegen, bijhouden en vernietigen van gegevens in het werkgebied van het programma. De verschillende gegevensbevoegdheden zijn dan ook "read", het recht om records in een object te lezen, "update" om records te wijzigen, "add" om records toe te voegen en "delete" om ze te verwijderen.
De object-management-bevoegdheid - het kunnen wijzigen van de bevoegdheden van gebruikers - kan zich richten op gebruiks- en gegevensbevoegdheid. Wanneer ze aan alle gebruikers zijn toegekend, worden ze public genoemd en in andere gevallen persoonlijk.
Men kent zowel "All" als "Normal" public bevoegdheden.
In het eerste geval kan een gebruiker het object gebruiken als ware hij eigenaar. Deze bevoegdheid wordt verleend door de eigenaar van het object. "Normal" omvat operationele bevoegdheid, nodig voor normaal gebruik. Hiervoor geldt per object een vaste combinatie. Ten aanzien van bestanden, bibliotheken en programma's heeft men uiteraard alle gebruiks- en gegevensbevoegdheden. Voor logische bestanden kan geen gegevensbevoegdheid worden verleend, omdat die geen eigen gegevens bevatten, maar altijd gegevens uit fysieke bestanden gebruiken.
CPF kan een programma laten lopen onder het gebruikersprofiel van de programma-eigenaar, wanneer tijdens het creëren de optie "user profile owner" is gebruikt. Dit eigenaarsprofiel wordt automatisch gebruikt door alle door dat programma opgeroepen programma's.
Een gebruiker moet beschikken over bevoegdheid om van een CPF object gebruik te kunnen maken. Datzelfde geldt voor het gebruik van de programmabibliotheek. Tijdens de creatie van een object moet worden aangegeven in welke bibliotheek het moet worden geplaatst. Wordt dit niet opgegeven, dan komt het object in de general purpose library, een standaardobject van CPF. Daarnaast kent het CPF standaard de systeem library en de tijdelijke programmabibliotheek.

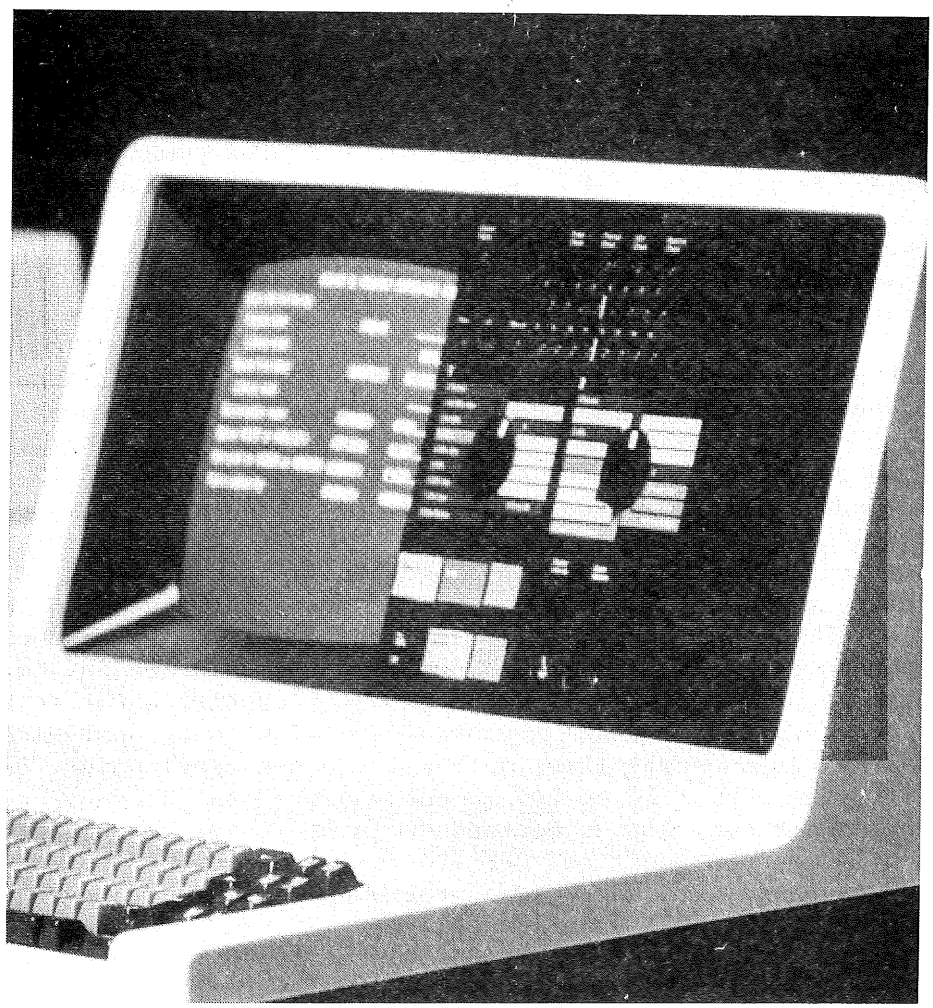
In tegenstelling tot het machine-interface laat het CPF geen vrijheid om objecten buiten een bibliotheek te houden.
Voor de security-mogelijkheden is het van belang dat een object uniek wordt gedefinieerd door een zogenaamde "qualified" naam, die bestaat uit de unieke naam van een object "gekwalificeerd" met de bibliotheeknaam. Hiervan kan gebruik worden gemaakt bij security contextwisselingen.

Realisatie beheersmodel met CPF

De afzonderlijke bedrijfsfuncties in engere zin, de systeembouwfunctie, de database-administratie, de security officer en de systeem operator zijn in het model afzonderlijke functies.
De operatorfunctie valt in een bedrijfsomgeving met uitsluitend online toepassingen vrijwel samen met de bedrijfsfuncties.
Tijdens de levenscyclus van een toepassing vallen ruwweg drie fasen te onderscheiden: bouwfase, acceptatiefase en operationele fase. De bouwfase bestaat uit het creëren van een database en de bouw van toepassingsprogramma's; dan komt de acceptatiefase en tenslotte de operationele fase.
Met behulp van de standaardobjecten van CPF kunnen deze drie verschillende contexten direct na het laden worden gerealiseerd.
Van belang is op welke manier de verschillende functies in concreto zijn verdeeld over organisatorische eenheden en personen. In de gekozen oplossing is ervan uitgegaan, dat de security officer, de systeembouw- en de database-administratiefunctie elk samenvallen met een organisatorische eenheid en dat daarnaast verscheidene afzonderlijke bedrijfseenheden bestaan met elk een eigen toepassingsgebied. De database kan door alle bedrijfsfuncties gemeenschappelijk worden gebruikt.
De twee hoofdobjecten van security-zorg zijn uiteraard de programma's en de database-bestanden.
Doel zal moeten zijn dat de database-administratie zekerheid heeft dat de operationele systemen in overeenstemming zijn met de afspraken over het gegevensgebruik, dat de eindgebruiker er zeker van is dat de geaccepteerde operationele systemen niet buiten zijn medeweten worden gewijzigd en dat de security officer weet dat geen voor de security relevante objecten aan zijn aandacht ontsnappen.
Dit betekent dat iemand, wil hij een object kunnen gebruiken, bevoegd zal moeten zijn voor het specifieke object en tevens voor de bibliotheek waar het te vinden is. Bovendien moeten alle contextwisselingen door de security officer worden beheerst. Deze laatste zal dan ook vier groepen bibliotheken creëren: voor de database-administratie, voor de systeembouw, ten behoeve van de acceptatietest en voor de operationele functies. Via het voor hem gereserveerde "create library" commando is hij automatisch eigenaar van alle bibliotheken en daardoor in staat het gebruik nauwkeurig te regelen. Door voor de bibliotheken slechts operationele bevoegdheden plus toevoeg- en ver-

wijderbevoegdheden te verstrekken en wel aan elke groep voor de bibliotheken van die groep, behoudt hijzelf het beheer erover. De database-bestanden mogen uitsluitend buiten het programma worden beschreven.

S 38 Console



Wanneer database-bestanden moeten worden gemaakt, creëert de database-administratie eerst een field reference bestand, waarin elk veld slechts éénmaal wordt opgenomen. Dit is een bronbestand, dat wordt gecreëerd met behulp van veldbeschrijvingen. Het bestand is de bron voor de creatie van een fysiek database-bestand.
Op basis van één of meer fysieke database-bestanden en een bronbestand kunnen één of meer logische database-bestanden worden gecreëerd. Voor de creatie van beide bestandstypen worden de opties "Level check yes" en "public authority none" gebruikt.
Zowel fysieke als logische bestanden moeten door systeembouw kunnen worden gebruikt en geplaatst worden in een systeembouwbibliotheek.

Hiervoor is operationele en toevoegbevoegdheid voor de bibliotheken nodig. Systeembouw is automatisch de eigenaar.
Systeembouwers creëren de gewenste programma's door eerst van de bestandsdefinities programmabronbestanden samen te stellen en die te compileren met behulp van het "Create RPG program"-commando of het "Create COBOL program"-commando.
Programma's worden gecreëerd met de optie "User program owner".
De creator moet operationele bevoegdheid hebben voor alle objecten, inclusief de logische en fysieke bestanden, waarnaar het programma verwijst. Daarnaast heeft hij ook de bevoegdheden om toe te voegen, te lezen, te muteren en te verwijderen. Als het programma gereed is voor gebruikersacceptatie, wordt het door de security officer overgebracht naar een testbibliotheek.
In dat geval krijgt alleen de eindgebruiker operationele bevoegdheid.
De security officer stelt met behulp van het commando "Display program reference" vast welke bestanden door het programma worden gebruikt.
De database-administrateur controleert of het de juiste bestanden zijn en brengt ze over naar de testbibliotheek. Omdat hij eigenaar is kan hij dit, mits hij operationele en toevoegbevoegdheid heeft gekregen van de security officer. Met behulp van het "clear file member" commando maakt hij deze gereed voor de acceptatietest. De gebruiker krijgt operationele bevoegdheid voor het te testen programma en de testbibliotheek. Omdat het programma is gecreëerd met de "owner"-optie, wordt het uitgevoerd zowel onder de bevoegdheden van het gebruikersprofiel als die van het eigenaarsprofiel. De eigenaar kan echter noch de programma's, noch de bestanden beïnvloeden. Omdat de bestanden zijn gecreëerd met de "Level check"-optie, wordt telkens bij de opening van de bestanden gecontroleerd of ze overeenstemmen met de externe bestandsdefinities op basis van het levelnummer. Dit bestaat uit datum plus tijd op het moment van creëren. Deze gegevens staan in het programma. Als de bestandsdefinitie later is gewijzigd, klopt dit niet meer en geeft het CPF een foutsignaal. Verloopt de acceptatietest naar wens, dan worden programma en bestanden overgebracht naar de operationele bibliotheek.
Als de database moet worden uitgebreid, bijvoorbeeld bij het creëren van een nieuw logisch bestand op basis van een operationeel fysiek bestand, kan het proces in omgekeerde richting plaatsvinden.
Het verschil is dat het operationele bestand gewoon moet blijven bestaan. Verhuizing is dus niet mogelijk. Kopiëren van een bestand is echter wel mogelijk met behulp van het "copy file" commando met de "create file yes"-optie.
De afzonderlijke testbibliotheek kan niet worden gemist, omdat er gedurende de testfase van een gewijzigd programma twee versies van een bepaald bestand moeten kunnen blijven bestaan.

Het resulterende bevoegdhedenschema is weergegeven in figuur 5.

Bibliotheek

Functie	DBALIB	PROGLIB	TESTLIB	PRODLIB
Sec.off.	eigenaar	eigenaar	eigenaar	eigenaar
DBA	operational +add+delete	operational +add+delete	operational +add+delete	operational +add+delete
Systeembouw	—	operational +add+delete	—	—
Eindgebruiker	—	—	operational	operational

Objecten

Functie	dba bestanden	programma's	gegevensbestanden
Sec.off.	all-object special	all-object special	all-object special
DBA	eigenaar	—	eigenaar
Systeembouw	—	eigenaar	operational + data
Eindgebruiker	—	operational	adopted systeembouw profile

Figuur 5. Bevoegdhedenschema.

Controlemogelijkheden van het CPF

De primaire doelstelling van een financiële of algemene controle (audit) is het verkrijgen van een oordeel over een financiële verantwoording. Onder de controlemiddelen zijn belangrijk: het zelfstandig onderzoek naar het cijfermateriaal, waaruit de verantwoording is opgebouwd én het zelfstandig onderzoek naar de organisatorische omstandigheden, waaronder dat cijfermateriaal is verzameld en verwerkt tot de te controleren verantwoording. Het onderzoek naar het cijfermateriaal kan in veel gevallen op doelmatige wijze geschieden met behulp van programmatuur, waarmee gegevensbestanden worden doorgeteld onder gelijktijdige selectie van records, die transacties of situaties (saldi) representeren, die voor een nader onderzoek in aanmerking komen. Die selectie

kan geschieden op basis van specifieke criteria of op basis van een mathematische steekproef. Waarneming van het totale bestand en verificatie van de volledigheid door middel van de totaaltelling is nodig om zeker te zijn dat alle samenstellende posten de selectiezeef zijn gepasseerd en gelijke kansen hebben gehad om voor nader onderzoek op de zeef te blijven liggen.
De wijze van realisatie biedt twee mogelijkheden. De eerste is, dat de accountant, in geval hij de beschikking heeft over een installatie, onafhankelijk van zijn cliënt het bestand kan onderzoeken met de beschikbare programmatuur. De cliënt zal dan het bestand op bijvoorbeeld diskettes of magneetbanden beschikbaar moeten stellen. Het Systeem 38 biedt beide mogelijkheden.
De tweede mogelijkheid is dat de accountant gebruik maakt van de installatie van de cliënt. In dat geval werkt hij evenals de reguliere gebruikers gelijktijdig met dezelfde installatie.
Dat betekent dat ook de accountant zijn eigen security context zal moeten hebben. Hij moet de redelijke zekerheid hebben dat binnen zijn context uitsluitend processen lopen op een wijze die door hem is gewenst en vastgesteld. Immers,hij moet zijn oordeel vormen op een van de cliënt onafhankelijke wijze.
Hoe zwaar dit punt in een praktijksituatie weegt en in hoeverre het onderzoek naar de kwaliteit van de organisatie een plaats inneemt in zijn controlewerkzaamheden, hangt onder meer af van de beschikbaarheid en toepassing van andere ondersteunende controlemiddelen.
Als hulpmiddel voor bestandsonderzoeken op de installatie van de cliënt kunnen in beginsel dezelfde programmeringshulpmiddelen worden benut als de cliënt zelf gebruikt. In elk geval komt RPG III in aanmerking.
Wil de accountant vaststellen of de organisatie berust op de juiste functiescheidingen en of de handhaving daarvan gedurende de controleperiode goed heeft gewerkt, dan moet hij weten hoe de security-organisatie is opgezet. De security officer zal hem via het beeldscherm de actuele security-organisatie kunnen tonen. Om te beoordelen of de informatie op de juiste wijze uit het Systeem 38 te voorschijn is gehaald, zal de accountant zich uiteraard moeten verdiepen in de gebruiksmogelijkheden van de machine, het CPF en de relevante commando's. De architectuur van het systeem en de wijze waarop het gebruik van de security-middelen in het CPF zijn gerealiseerd, staan er redelijkerwijs borg voor, dat het uitvoeren van een bepaald commando ook de voorspelde uitkomst zal opleveren. Als aanvulling zal de accountant proberen vast te stellen hoe de security gedurende de controleperiode heeft gewerkt. Voor de tijd waarbinnen hij zelf voor zijn controle van de machine gebruik heeft gemaakt, zal dit zwaarder wegen dan voor de gehele periode waarover de controle zich uitstrekt. De voor het eerste geval benodigde informatie kan worden ontleend aan de logging van de machine. De manier waarop de logging is ingebed in het machine-interface en het CPF, maakt de risico's dat de accountant een onvolledige logging te zien krijgt, gering.

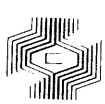
Of de logging van wijzigingen in de security-context volledig is, moet berusten op procedurele maatregelen. Het is immers mogelijk de machine van tijd tot tijd opnieuw te initialiseren.
In beginsel bestaat de mogelijkheid dat de logging van een bepaalde periode niet wordt overgelegd, zonder dat dit duidelijk blijkt. Wat wel kan blijken is het ontbreken van logging-informatie over een periode waarvoor op andere wijze is vastgesteld, dat de machine in die periode moet zijn gebruikt.

Conclusie

Het Systeem 38 biedt door zijn principieel op capabilities gebaseerde architectuur, mogelijkheden voor het treffen en beheersen van goede security-maatregelen. Deze mogelijkheden waren tot nu toe slechts op experimentele machines beschikbaar.
De machine- en CPF-ondersteuning van database-functies biedt een behoorlijk instrumentarium voor de database-administrateur als beheerder en bewaker van de nakoming van afspraken over het gemeenschappelijk gegevensgebruik.
De displaycommando's bieden op elk moment de gelegenheid kennis te nemen van de actuele status van de security-organisatie en het database-gebruik.
Door de stringente security-faciliteiten is de accountant in staat om, zonder verlies van zijn onafhankelijkheid, voor zijn bestandsonderzoeken van de installatie van de cliënt gebruik te maken.
Voorwaarde voor de accountant is echter dat hij zich de benodigde kennis van het systeem eigen maakt. Dat is echter niets bijzonders. Hij zal immers vrijwel steeds kennis nemen van de organisatie, waarbinnen een door hem te controleren verantwoording tot stand komt.
De eenmaal door hem verworven kennis van het Systeem 38 is in elke omgeving, waar hij de machine tegenkomt, te gebruiken. Een belangrijke reden daarvoor is het bestaan van in beginsel slechts één CPF. De Systeem 38 gebruiker heeft niet de vrijheid om bepaalde delen van het CPF wel of niet te genereren. De accountant zal dus steeds overal een compleet CPF aantreffen.

Referenties

1. IBM Systeem 38 bibliografie GH 30-0233.
2. Hamacher e.a. Computer organization, McGraw Hill, 1978.
3. Linden T.A. Operating system structures to support security and reliable software, Computing Surveys Volume 8, no. 4 December 1976.
4. Houden, M.E. e.a. IBM System 38 support for capability based addressing, Proceedings 8th annual symposium on computer architecture 1981 (ACM, IEEE).
5. Berstis, V. Security and protection of data in the IBM System 38, Proceedings 7th annual symposium on computer architecture 1980 (ACM, IEEE).



BOEKEN

Door J. Philippo

AC 347 "Fraude, automatisering en accountant" een uitgave van het Limperg Instituut. 1981.

Deze publikatie vormt de neerslag van een op 6 januari 1981 te Amsterdam gehouden studiedag voor accountancy-studerenden over het thema "Fraude, automatisering en accountant".

De genoemde studiedag was een initiatief van de in Amsterdam gevestigde Vereniging van Accountancy-Studenten (VAS).
Contacten tussen het VAS-Bestuur en de Wetenschappelijke Raad van het Limperg Instituut leidden tot de conclusie, dat het wenselijk moest worden geacht het materiaal, dat die dag zou opleveren, te publiceren. De overwegingen daarvoor waren het belang van het onderwerp, de samenstelling van het team van inleiders en de schaarse Nederlandstalige literatuur op dit punt.
Een nauwe samenwerking tussen VAS, inleiders en Limperg Instituut leidde tot de voorliggende publikatie.

Als inleiders traden op representanten van de accountant in de controlerende en in de adviserende functie, van het bedrijfsleven en van de financiële pers.
Theoretische beschouwingen en praktijksituaties inzake fraude, zowel met als zonder computer, kwamen op de studiedag aan de orde. Het boek geeft deze inleidingen weer. De eerste vier inleidingen van de hand van de heren Brugge, Frielink en Veenis richtten zich op het verschijnsel fraude en de taak van de accountant, waarvan vooral de twee artikelen van de heer Frielink zeer lezenswaard zijn.
Een volgend viertal artikelen betreffen de automatisering. Hieronder valt ook de inleiding van de heer Huesmann over de fraude bij zijn eigen organisatie, terwijl de heren Neisingh en Gerritse de topic automatisering en controle respectievelijk de opleiding daarvoor bespreken.

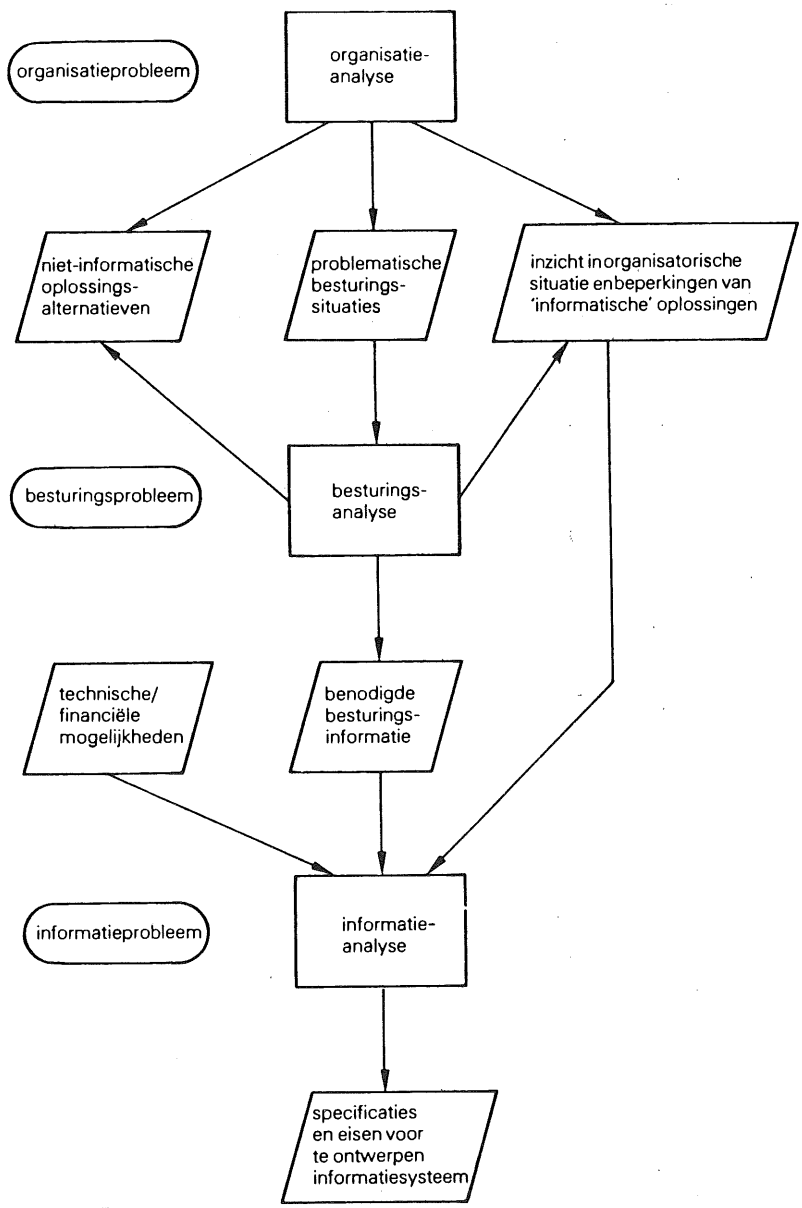
In de bijlagen is een aantal voor het onderwerp belangrijke publikaties opgenomen, waaronder de weergave van de - zij het beperkte - enquête gehouden door het VAS over dit onderwerp bij het bedrijfsleven.
Een weergave van de paneldiscussie voltooit het beeld over de op de studiedag behandelde materie.

Het boek, dat voor studerenden tegen gereduceerde prijs bij de VAS verkrijgbaar is en voor anderen bij het NIvRA voor *f* 25,--, is een welkome bijdrage op dit gebied.

AC 346 "Informatiesystemen" onder redactie van
dr.ir. N.J.T.A. Kramer. 1981
Uit de serie NOVI-serie leerboeken informatica (Kluwer).

Dit boek bevat een gedeelte van de leerstof voor de module S4 van de AMBI-opleidingen, namelijk de informatie analyse en het voorliggende terrein van organisatie-analyse en besturingsanalyse, het geheel gericht op de informatievoorziening in een organisatie.

Informatievoorziening is zodanig verweven met het totale gebeuren in de organisatie, dat het niet mogelijk is de informatievoorziening onafhankelijk van de andere aspecten - dan alleen de informatie-analyse - te beschouwen.
Samengevat ziet deze gedachtengang - welke het kader van het boek vormt - er als volgt uit:



Het proces van organisatie-, besturings- en informatieanalyse.

De eerste hoofdstukken omvatten de volgende onderwerpen:

- organisatievraagstukken, welke rechtstreeks gekoppeld zijn aan de informatieverzorging in organisaties, zoals voor besluitvorming en onzekerheidsreductie;

- het besturen van organisaties vanuit de bedrijfseconomische bedrijfsvoering;

- de systeemleer, welke het begrippenkader en de methode biedt voor beschrijving en het onderzoek van de besturingsproblematiek.

De voornoemde hoofdstukken geven de basis waarop aan de analyse van organisatie- en besturingsproblemen gestalte kan worden gegeven; de hoofdstukken 5, 6 en 7 gaan over de informatie-analyse in engere zin en het daaruit resulterende logisch ontwerp van een informatiesysteem met als onderwerpen:

- theoretische aspecten van informatiesystemen en het begrippenkader voor beschrijving van informatie en de wijze van analyse;

- informatieprecedentenanalyse als taal voor het specificeren van de inhoud van informatiesystemen. De precedentenanalyse is een hulpmiddel om gegevensverzamelingen, processen en relaties te specificeren zonder uitspraken te doen over de technische of organisatorische oplossing daarvan;

- praktische aspecten met eisen waaraan informatievoorziening en -verwerking organisatorisch en technisch moet voldoen alsmede de consequenties voor de realisering voor het informatiesysteem.

Uit het voorgaande zal het duidelijk zijn dat slechts een gedeelte van de problematiek van informatiebehoeften worden behandeld. Niet naar voren komen de onderstaande onderwerpen, welke tevens tot de leerstof voor de S4 module behoren:

- typen organisaties en hun informatiebehoeften;
- informatiebehoeften in verschillende functies;
- kenmerken van informatiesystemen.

De module S4 van de AMBI-opleiding richt zich op de vaardigheden in het bepalen en ordenen van de informatiebehoeften alsmede het verkrijgen van inzicht in het logisch ontwerp van informatiesystemen - het werkterrein van de informatie-analist. Voor de EDP-auditor als kritisch waarnemer van dit werk wordt het boek ook aanbevolen.

LITERATUUR

door J.C.P.M. Vermeeren en drs. B.M. de Vries

Computer security and integrity
Problems and prospects

Cadambi A.
Srinivasan and
Paul E. Dascher

Info Systems; mei 1981
excerpt: Edpacs August/September 1981

Het hierna opgenomen excerpt geeft een vrij volledig overzicht van het "automatisering en controle"gebied. In die zin is het artikel niet zonder belang voor alle bij automatisering betrokken accountants. Om die reden nemen wij het graag in deze rubriek op.

COMPUTER SECURITY AND INTEGRITY: PROBLEMS AND PROSPECTS, by Cadambi A. Srinivasan and Paul E. Dascher. Infosystems, (Hitchcock, Publishing Co., Hitchcock Building, Wheaton, IL, 60187). May 1981; pp.116, 118, 121-123.

Top management is beginning to realize the need to implement security measures and countermeasures in computer systems. Published cases and incidents make it clear that outsiders as well as trusted employees can penetrate and manipulate systems that are not adequately secured. Information security involves three separate, but related, issues:

- Confidentiality. Data must be protected against disclosure to unauthorized users.
- Integrity. Data must be protected against unauthorized or erroneous destruction or alteration. Further, it must be protected from unauthorized use.
- Availability of service. Systems must be protected to preclude malicious denial of services to authorized users.

Existing technology provides confidentiality safeguards, but the other two issues do not have satisfactory solutions.
Management should recognize the need for computer security and establish a security policy coordination function with the following responsibilities:

- Develop workable security standards.
- Coordinate the acquisition/implementation of security countermeasures.
- Ensure the reliable operation of countermeasures.
- Develop contingency plans.
- Plan and conduct tests of countermeasures.

Basically, the security coordination function performs a risk analysis to select the most effective countermeasures and works with the audit function to verify the adequacy of the countermeasures that are implemented.
The technology that supports secure computer systems is based on the following:
- A system development life cycle that emphasizes reliability.
- System architecture that assigns security responsibility to specific hardware and software units and then protects them from security violations.
- The use of encryption to protect data transmission.

DATA SECURITY COUNTERMEASURES.
There are two categories of security safeguards: prevention and detection. Preventive measures try to preclude security violation incidents. Detection controls reveal the occurence of security violations and point the way toward corrective action. In most cases, detection safeguards operate on an after-the-fact basis.

PREVENTION SAFEGUARDS.
- Provisions to detect and extinguish fires.
- Access control procedures.
- Personnel practices.
- Password protection.
- Input/output data and storage control.
- Program change controls.
- System testing and documentation procedures.
- Verification of application system design.

DETECTION SAFEGUARDS.
- Physical surveillance of the operational area.
- Alarm systems.
- Logs of:
  . User commands.
  . Access to sensitive files.
  . Operator console actions.
  . Data transformations.
  . Media usage.
- Audits of:
  . Computer resource usage.
  . Data handling.
  . Selected transactions.
- Audit techniques employed:
  . Use of test data.
  . Generalized audit software.
  . Snapshot.

DEFINITION OF AN AUDIT.
An audit is an independent and objective review of an EDP system. Its objectives can be defined as follows:

- Reviewing the existing system to detect security weaknesses.
- Utilizing existing system trails to monitor and deter threats to security.
- Assuring individual accountability.

A security audit designed to achieve these objectives is performed at three levels:

- System Audit. An analytical review that covers all aspects of system design in order to assess the adequacy of controls and evaluate compliance with the organization's standards.
- Software Audit. A review to assure software quality. Such reviews usually promote the uniform, standardized design of software, but they are not concerned with the validation of the programs.
- Threat Monitoring. A review and analysis of logs and other audit trails to detect events that might represent security violations.

IMPLEMENT SAFEGUARDS.

Four factors are central to the effective implementation of system-based security safeguards: identification, authorization, audit of access, and data encryption. The first three will be discussed here.

1. Identification. Accurate identification of users is essential to accountability, a key element in computer security. Identity is established in one of three ways:
   - Something a person knows (e.g., a password).
   - Something a person has (e.g., a badge or key).
   - Something unique to a person (e.g., signature or fingerprints).

   To date, the password is the most cost-effective method of personal identification. The user is not the only systems element that must be identified. Hardware devices, programs, and data sets should all have unique names and, when appropriate, version numbers that can establish their identity.

2. Authorization. When a user or other system element has been identified, the security scheme must then establish the extent of that user's authority. To provide an effective level of security, each user should be given the lowest level of privilege required to perform his authorized tasks.

   A formal authorization process is based upon the following elements:
   - A set of valid users.
   - Unique identification of users.
   - A set of system resources (e.g., programs, data files, hardware units, etc.).
   - Data needed to verify resource identify.
   - A definition of the authorization relationships between users and resources.

   System authorization can be expressed at various levels of detail. A fine level of detail makes it easier to detect security violations, but it tends to increase processing overhead and degrade system performance.

Security provisions should be simple and rigid in order to limit oversights and human error. On the other hand, flexibility and selectivity are important to the efficient operation of a system. To accomplish these conflicting objectives, the trend seems to be toward a security system that sets and enforces an overall access control framework within which an owner of a resource or function can delegate access authority to another user.

3. Auditing Access. A log provides a limited set of facts about access to data. A complete record of data activity is maintained on a journal that can be utilized to reconstruct a data base. An audit review of the log should uncover details about possible security violations. As a result, the log should be a secure file. A special computer program may be used by the auditors to abstract data from the log. Access to this program should also be controlled.
Logging is usually performed after the verification of authorization. A special log of rejected accesses should be kept. This log should be reviewed and evaluated on a timely basis. Some useful information to be captured for post audit review is:
   - Access information.
   - Records that trace data through creation, update, and destruction.
   - Records of changes to the access control parameters.
   - Records of operator and security officer actions.
   - Records of rejected access attempts.

ROLE OF THE AUDIT.
A security audit satisfies two requirements:
- As a defensive measure, it determines the response to the discovery of improper data usage.
- It provides surveillance over security violation attempts and initiates countermeasures.

These efforts on an on-going basis are necessary to assure the adequacy of access controls.

OBSERVATIONS.
This article furnishes some general observations about physical security and access controls within EDP systems:
1. Available security measures are adequate to protect computer installations.

2. New techniques for identification and authentication are being developed.

3. Improved cryptographic techniques will provide better levels of communications security.

4. Emphasis on quality assurance will make software more reliable and improve documentation.

5. The cost of inadequate security can be very high.

6. Advances in computer technology make it possible to pursue the design of systems that will provide effective security, reliable software, and efficient operating performance.

Turning up the control — Brian Matthews

Accountancy age January 1980
Uittreksel: Edpacs August/September 1981

Gezien het toenemende gebruik van de computer bij de accountantscontrole en de voordelen daarvan is het goed ook eens bij de risico's stil te staan.

In dit artikel (samengevat in onderstaand excerpt) worden de maatregelen besproken om de risico's verbonden aan het "interrogation process" van "computerized accounting systems" te mitigeren.

On a routine basis, auditors employ computer audit software to interrogate computerized accounting systems. This article looks at the controls that should be applied to this interrogation process. The need for such control is often overlooked.
The auditor's objectives in using such software are:
- Provide a method for bridging gaps in the audit trail.
- Test for compliance with control procedures.
- Investigate the consequences of known weaknesses in internal control.

All these objectives involve looking for both error and fraud. There is a concern that the client's staff might be able to thwart the auditor's efforts. Adequate control over the interrogation process will reduce this risk.
The auditor should be skeptical of any client-produced data provided to support the financial statements. However, he might not have to be so cautious if the data was produced under his control.
How can the specifications for an interrogation be corrupted by an error? The possibilities are countless, but three are both common and serious:
- Failure to produce control totals that will verify that all the data has been processed.
- Use of exception reporting is a risky technique for audit applications. A minor error in parameter specifications could cause the auditor to miss some significant transactions.
- Incorrect definition of the data file. Such an error might be a mistake by the auditor or the result of an error or changes in the client's file layouts. While such errors can happen quite easily, they are very difficult to detect.

The auditor can reduce errors by the use of detective audit control techniques. This involves control features that provide evidence that the audit program's logic was correct. For example, when selecting items from a file, the interrogation program can produce control totals of both selected and unselected records. These control totals can be checked against the overall totals for the file or files involved.
Developing detective audit controls can be a difficult task. The following general rules may make the job simpler:

- Control totals should be generated by program logic which is separate from the logic used to select transactions.
- Totals must provide verification that all records have been processed.
- Totals should account for the effect of file reduction or data rejection logic. This involves the use of "before" and "after" counts or control totals that can be used to reconcile to original controls.
- Audit control totals should reconcile to client totals. All interrogation reports must be proven to show they are based upon the same data that was used to prepare the financial statements.

The auditor must also protect his interrogation process against deliberate interference. This involves a number of additional considerations.
What are the risks? The auditor must try to think like someone who wants to thwart the audit process. For example, consider a computer operations manager who has been exploiting a control weakness in the purchasing system. In collusion with the purchase ledger supervisor, the operations manager has been generating and diverting payments for non-existent services. The auditors are going to use an interrogation program to select purchase transactions.
Since he cannot remove the fraudulent transactions from the file without throwing the controls out of balance, the manager would like to make sure his items are not chosen. Because he is unable to obtain access to the logic of the auditor's software, he cannot tamper with the selection process. However, all is not lost.
All printed reports within the installation are produced from a "spool" file. The manager does know how to access this file from a remote terminal. He can alter any selected transactions that are related to his fraud before they are printed on the auditor's output report. To provide a solid margin of time to accomplish these alterations, the manager can make sure the "spool" file is quite full before the audit application is processed.
To avoid manipulations like the one described, the auditor must carefully evaluate the risks involved in each applications. Some effective control techniques include:

Input Phase

- Check all data entry processing performed by the client against original audit interrogation specifications.
- Do not give the computer operator the interrogation parameters until the processing run has been started.
- Reload the interrogation system each time it is used.
- Erase all audit disc files at the end of each run.

Processing Phase

- Do not let the client have access to any source code generated by the interrogation program. This may mean the development and testing will have to be done at another site.
- Make sure the operating system is maintaining complete records of run times, operator actions, input and output file activity, and other occurrences.
- If there are any doubts about processing integrity (e.g., because of online terminal facilities), consider using another site for audit processing.

Output Phase

- Make at least one change in report format each time an interrogation is processed. This makes it impossible for anyone to use a previous run as the basis for imitating an audit report.
- If there is any possibility that the printer "spool" could be altered, do not produce hardcopy reports.
  Encipher output data and write it to a magnetic tape. Deciphering and printing can be done later at another site.
- Make sure all output files are overwritten or erased when audit processing has been completed. The client should not be able to determine what transactions have been selected for detailed review.

If the use of the controls outlined in this article becomes too burdensome, it is probably not cost-effective to continue processing at the client's installation. The auditor should move to an independent facility.

The interrogation of very complex files (e.g., a database) presents some additional problems. Audit interrogation software may not be able to access the data. Auditors usually feel they will have to accept some loss of independence and rely on client personnel to extract data in a sequential format.

Does this approach really involve a loss of independence? Not necessarily. The auditor must still total the file, retain control over the data processed, and agree control totals to the client's records. In the final analysis, a sequential extract file from a data base is no different than, and can be relied upon as much as, any file produced by a client.

This same basic logic can be applied to the inclusion of client file handling routines within an auditor's software. Properly handled, the use of such routines does not cause a loss of audit control. However, the auditor should be the one who integrates the file handler into his software.

Audit control of computer interrogations is a subject that needs careful consideration. It sometimes appears to involve difficult problems, but these can be solved by the use of basic audit control principles. Independent proof of the data processed is the key element.

Confidentiality of Information — H. Roos R.A.

Information & Management 4 (1981)

De relatie tussen de organisatiestructuur, de daarvoor ontwikkelde toepassingssystemen en het onderwerp vertrouwelijkheid van informatie leiden tot een verantwoordelijkheid voor informatiebeheersing bij de eindgebruikers.

In omgevingen waar gemeenschappelijk gebruik van gegevens voorkomt kan die verantwoordelijkheid niet meer door de individuele eindgebruiker gedragen worden. Daarom zal de gemeenschappelijke verantwoordelijkheid van de gebruiker voor de gemeenschappelijke gegevens geregeld moeten worden in een "overeenkomst".

De aangewezen functionaris om op de naleving van deze "overeenkomst" toe te zien lijkt de data base administrator. Iedere afwijking van c.q. leemte in de preventieve controlemaatregelen verzwakt deze "data sharing control".

Gegeven de huidige machine-architectuur kan de controle met behulp van toegangsbeveiligingstabellen worden doorbroken. De daaruit voortvloeiende leemten ten aanzien van de bewaking van gemeenschappelijke gegevens dienen te worden gecompenseerd door organisatorische en procedurele maatregelen.

Information systems audit — Keagle W. Davis

Management accounting, maart 1981

In "Uit het Buitenland" (vanaf pag. 181) troffen wij een artikel aan over "information systems audit" van Keagle W. Davis uit Management Accounting van maart 1981.

Volgens de korte inleiding bij dit artikel voorspelt de auteur in zijn artikel, dat in het komende decennium "EDP-auditors" zich zullen ontwikkelen tot "information system auditors". Het artikel bevat echter een beschrijving van de aanpak van een toepassingssysteembeoordeling, waarbij nadruk gelegd wordt op de voorbereiding en systematiek van de aanpak.

De accountant wordt, ten gevolge van de snelle technologische ontwikkelingen in de komende jaren geconfronteerd met een aantal problemen:

1. de accountant wordt meer en meer verantwoordelijk gesteld voor de interne controlemaatregelen en de documentatie ervan;
2. het definiëren van de interne controlecriteria dient onderdeel te zijn van de normale systeemontwikkelingsstandaarden;
3. de controlemethodiek en de documentatie hiervan moet worden verbeterd.

Deze problemen zijn zowel vaktechnisch als economisch.

- Vaktechnisch, omdat de accountant tot taak heeft de interne controlemaatregelen met behulp van de documentatie te onderzoeken en te beoordelen in plaats van de interne controlemaatregelen zelf te definiëren en vast te leggen, om ze vervolgens te beoordelen.
- Economisch, omdat het zelf verzamelen en documenteren veel tijd en geld kost. Daarom zal onderkend moeten worden, dat deze kosten niet tot de normale controleactiviteiten van de accountant behoren, maar een vorm zijn van ondersteuning van de cliënt in het samenstellen van gebruikers- en systeemdocumentatie.

Naarmate geautomatiseerde systemen in omvang en in complexiteit zijn gegroeid en alleen nog op elektronische wijze met elkaar zijn gekoppeld, liggen de verantwoordelijkheden voor de interne controlemaatregelen niet meer duidelijk vast. Het is thans gemeengoed, dat meerdere afdelingen binnen de organisatie dezelfde gegevens gebruiken, terwijl zij ieder hun eigen zorgen hebben over juistheid, tijdigheid en volledigheid van deze gegevens.

Een ander probleem is de behoefte aan een evaluatiemethodiek van interne controlemaatregelen, die zichzelf documenteert en die inzichtelijk is.

De oplossingen voor de problemen, zowel van vaktechnische als van economische aard, zijn drieledig.

a. ontwikkeling van een betere controlemethodiek;
b. bevorderen van de participatie van de accountant bij het opstellen van verbeterde systeemontwikkelingsstandaarden;
c. het terugbrengen van de verantwoordelijkheden naar waar zij behoren: bij de gebruikers, de automatiseringsafdeling en bij de leiding.

Controlemethodologie begint met de top down benadering

Alvorens te beginnen met het onderzoek per applicatie, zal inzicht in het geheel van de gegevensverwerking inclusief de korte en lange termijnplannen verkregen moeten worden door middel van een benadering, welke omvat:

1. The overall EDP system structure:
   a. hardware and online network;
   b. system and data management software and how it impacts applications;
   c. existing major applications with indications of financial and operational impact;
   d. short and long-range hardware and software development plans.
2. The process and standards used for systems development and maintenance; and how the systems environment can impact the development and maintenance process and consequently the applications themselves.
3. The major applications which are (or soon will be) under development and those which will be replaced. For each, there should be high level documentation including:
   a. an overview systems narrative;
   b. a high level flowchart of the hardware, software and terminals by location;
   c. applications/transactions which are processable at each location.

Alleen op grond van deze top-down-benadering kan de EDP-auditor op logische wijze de korte en lange termijn controleplannen ontwikkelen. Op grond van deze benadering dient de accountant een totaal beeld te hebben van de risico's, verbonden aan iedere applicatie.

De control evaluation methodology

De accountant is veelal geneigd om alle maatregelen van interne controle, risico's en controledoelstellingen te onderzoeken, in plaats van het onderzoek te richten op de in relatie tot risico's en controledoelstellingen belangrijkste interne controlemaatregelen.

De control evaluation methodology heeft de volgende uitgangspunten:

1. De risico's, welke zich op elk niveau van de organisatie voordoen, kunnen naar kans van optreden worden gerangschikt.
2. Elke organisatie en systeem bestaat uit een aantal functies, welke op hun beurt een aantal activiteiten, zowel handmatig als geautomatiseerd, omvatten. Per activiteit wordt aangegeven, wat fout kan gaan. Hiervan uitgaande kan vastgesteld worden, welke interne controlemaatregelen ten opzichte van deze fouten en risico's dienen te worden genomen.
3. De interne controlemaatregelen, welke afgestemd dienen te worden op de controledoelstellingen en op de risico's per activiteit, variëren sterk voor wat betreft hun efficiency en effectiviteit.

Tijdens de keuze zijn 3 factoren van belang:
- type of control: preventive
  detective
  corrective
- how applied:
  . discretionary; dit zijn maatregelen van interne controle, die niet permanent worden toegepast;
  . non-discretionary, maatregelen van interne controle, die permament en op dezelfde wijze worden toegepast.
- method of implementation:
  . EDP;
  . manual.

De methodology is weergegeven in de control matrix (figuur 1).

Uit een analyse van de te nemen interne controlemaatregelen (zie figuur 2) blijkt, dat:

- de "preventive, discretionary" (preventieve, en niet-permanent toegepaste) maatregelen van interne controle slechts in beschei-den mate effectief zijn.
- de "detect/corrective, non discretionary" (repressieve controle-maatregelen aangevuld met corrigerende maatregelen, welke perma-nent worden toegepast) maatregelen hoogst effectief zijn (bij-voorbeeld een geprogrammeerde controle met suspense file).

Control evaluation matrix

De control evaluation methodology kan op systematische wijze worden toegepast door gebruikmaking van de control evaluation matrix (zie figuur 3).
Met behulp van deze matrix kunnen de meest effectieve maatregelen van interne controle per activiteit worden geselecteerd. In de matrix wordt ook het resultaat van het uittesten van de controlemaat-regel vastgelegd, waardoor inzicht in de werking wordt verkregen.
De schrijver stelt, dat niet de accountant, maar de gebruikers en automatiseringsfunctionarissen deze documentatie dienen samen te stellen, waarvoor begeleiding en voorlichting vereist is.

Verbetering van het proces van begeleiding en voorlichting

Benadrukt wordt, dat systeemontwikkeling en EDP management meer con-trol-minded moeten worden gemaakt door opleiding op het gebied van de controlepraktijk. Het opnemen van een systems quality assurance-functie wordt aanbevolen.
De gebruikers dienen opleiding te ontvangen op het gebied van systeemontwikkeling, -onderhoud en van controlemaatregelen op appli-catieniveau.
In het management zullen mensen met kundigheden op het gebied van system audit moeten worden opgenomen.

De EDP auditor zal zijn automatiseringskennis van EDP moeten uitbreiden, wil hij kunnen fungeren als "information systems auditor" van de 80er jaren. Onder de opleiding van de EDP auditor horen o.a.:

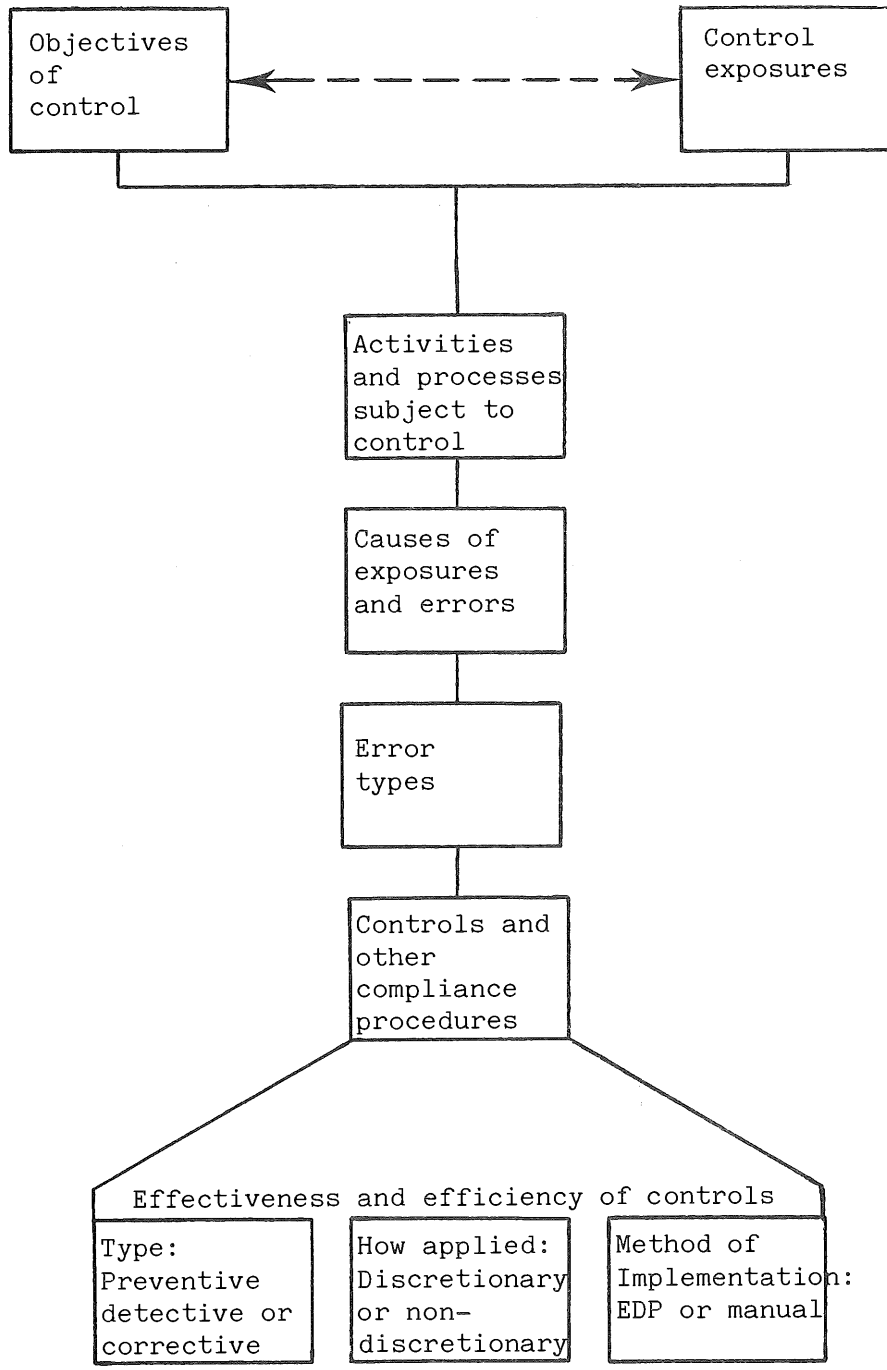
- tenminste een aantal dagen opleiding in on-line-systemen en in terminalcontrols;
- aantal dagen introductie in de structuur van een database vanuit conceptueel gezichtspunt en 3 of meer dagen opleiding in de bijzonderheden van een database systeemtoepassing.

Ter afsluiting geeft de schrijver de volgende waarschuwing.

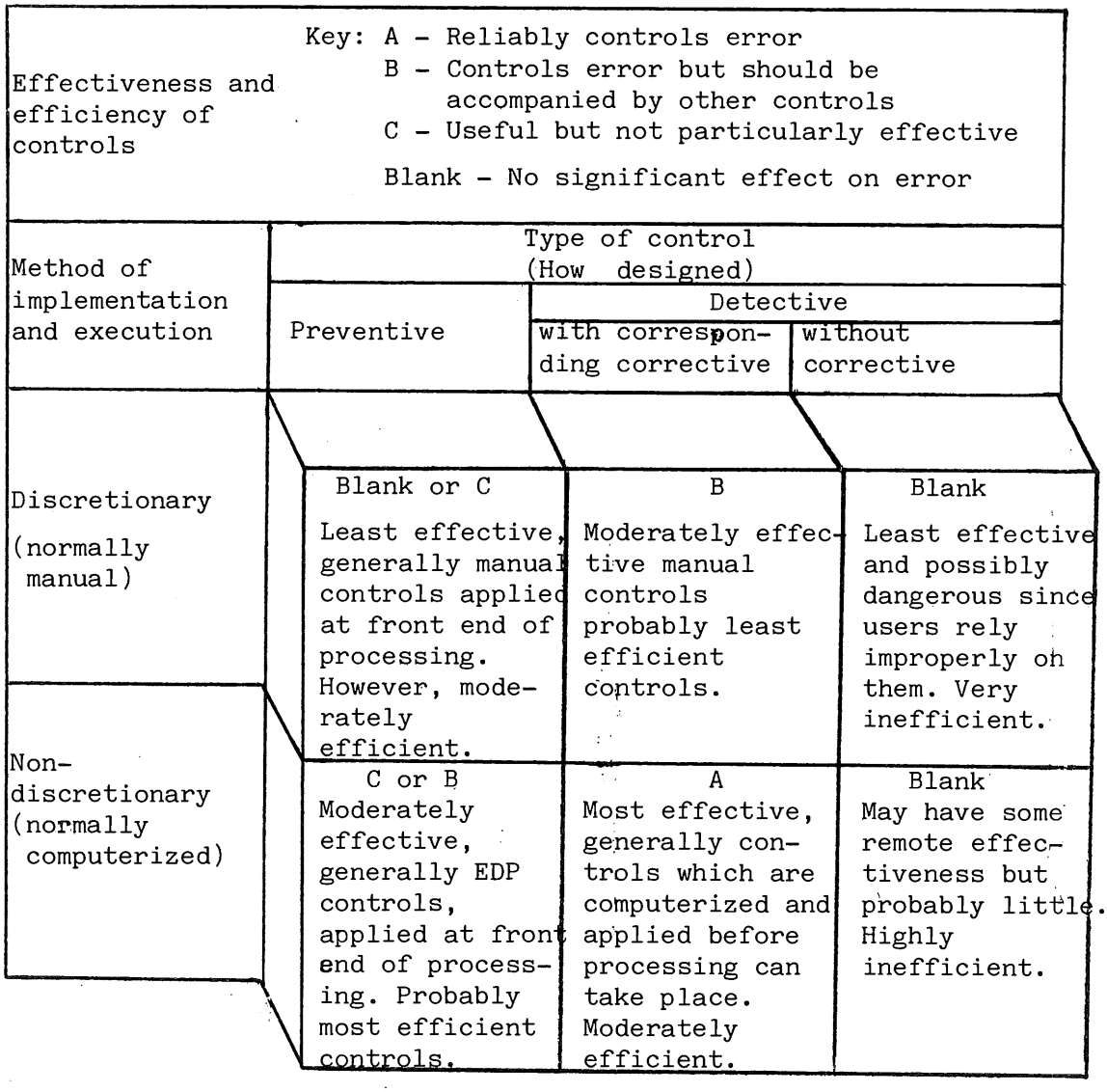
As we progress into the 1980s with micros and minis upon us and overwhelming budgetary pressures of EDP and ourselves, we must remember one thing: the prerequisite for well controlled systems in the future is adequately trained data processing personnel who have a knowledge of controls, and users and management personnel who have a knowledge of systems development and controls. Unless users and managers take the primary responsibility for controls in their own systems and implement those controls, the job of the information systems auditor in the 1980s will be overwhelming.

Figuur 1

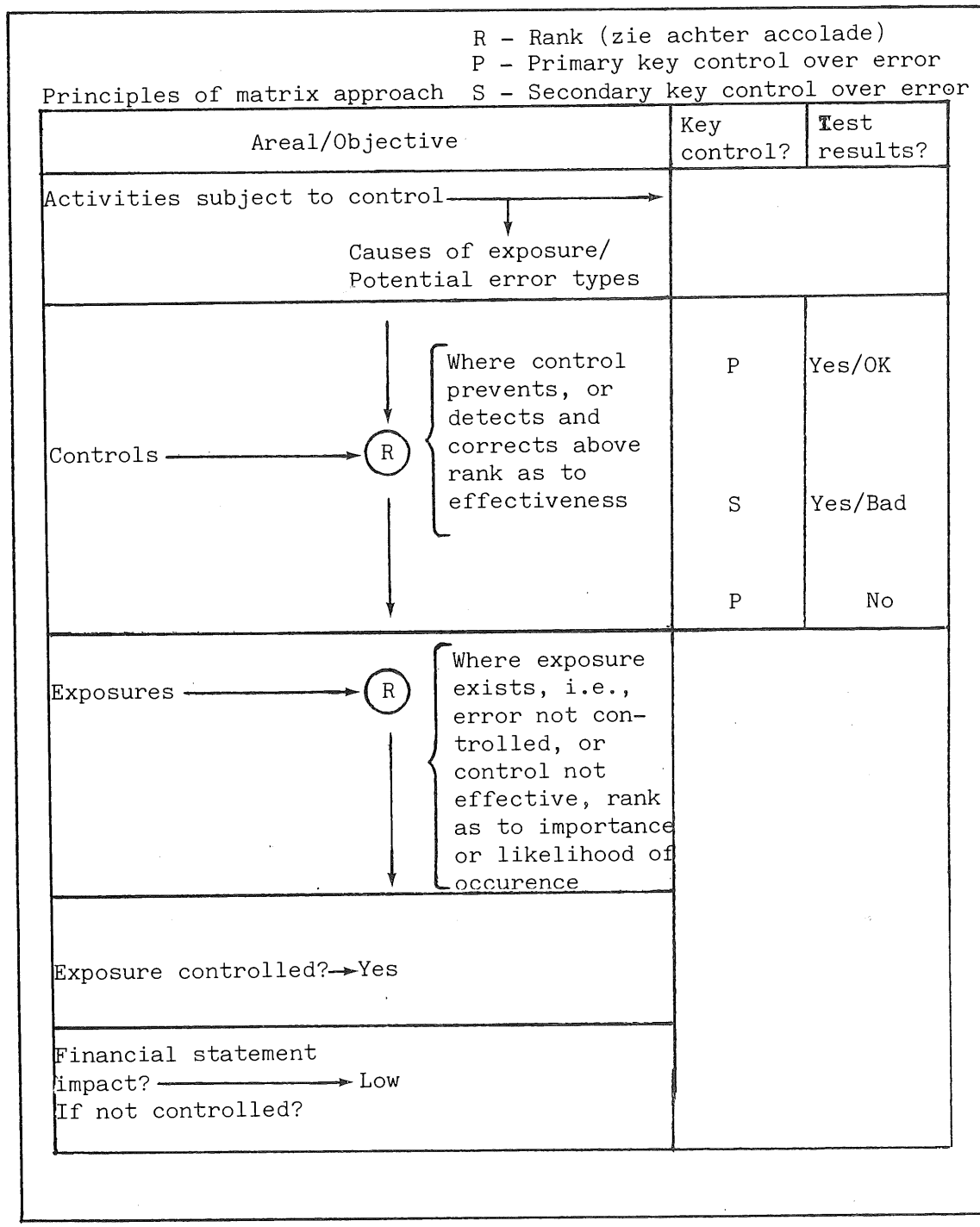
Basic concepts of a control matrix.



Figuur 2


Key: A - Reliably controls error
B - Controls error but should be accompanied by other controls
C - Useful but not particularly effective
Blank - No significant effect on error
Effectiveness and efficiency of controls
Method of implementation and execution
Type of control (How designed)
Preventive
Detective
with corresponding corrective
without corrective
Discretionary (normally manual)
Blank or C
Least effective, generally manual controls applied at front end of processing. However, moderately efficient.
B
Moderately effective manual controls probably least efficient controls.
Blank
Least effective and possibly dangerous since users rely improperly on them. Very inefficient.
Non-discretionary (normally computerized)
C or B
Moderately effective, generally EDP controls, applied at front end of processing. Probably most efficient controls.
A
Most effective, generally controls which are computerized and applied before processing can take place. Moderately efficient.
Blank
May have some remote effectiveness but probably little. Highly inefficient.

Figuur 3


R - Rank (zie achter accolade)
P - Primary key control over error
S - Secondary key control over error
Principles of matrix approach
Areal/Objective
Key control?
Test results?
Activities subject to control
Causes of exposure/
Potential error types
Controls
R
Where control prevents, or detects and corrects above rank as to effectiveness
P
Yes/OK
S
Yes/Bad
P
No
Exposures
R
Where exposure exists, i.e., error not controlled, or control not effective, rank as to importance or likelihood of occurence
Exposure controlled?→Yes
Financial statement impact? → Low
If not controlled?

Computer Graphics: A Reporting Revolution ? Irwin M. Jarret CPA

Journal of Accountancy, May 1981

De ondertitel van dit artikel "Using charts as a primary medium for presenting financial data" en de constatering dat dit door de toenemende automatisering mogelijk (= betaalbaar) wordt, is voldoende aanleiding om in deze rubriek aandacht te besteden aan dit artikel.

In beide onderstaande voorbeelden wordt een geheel grafisch samengestelde balans en resultatenrekening gegeven.

Exhibit 1

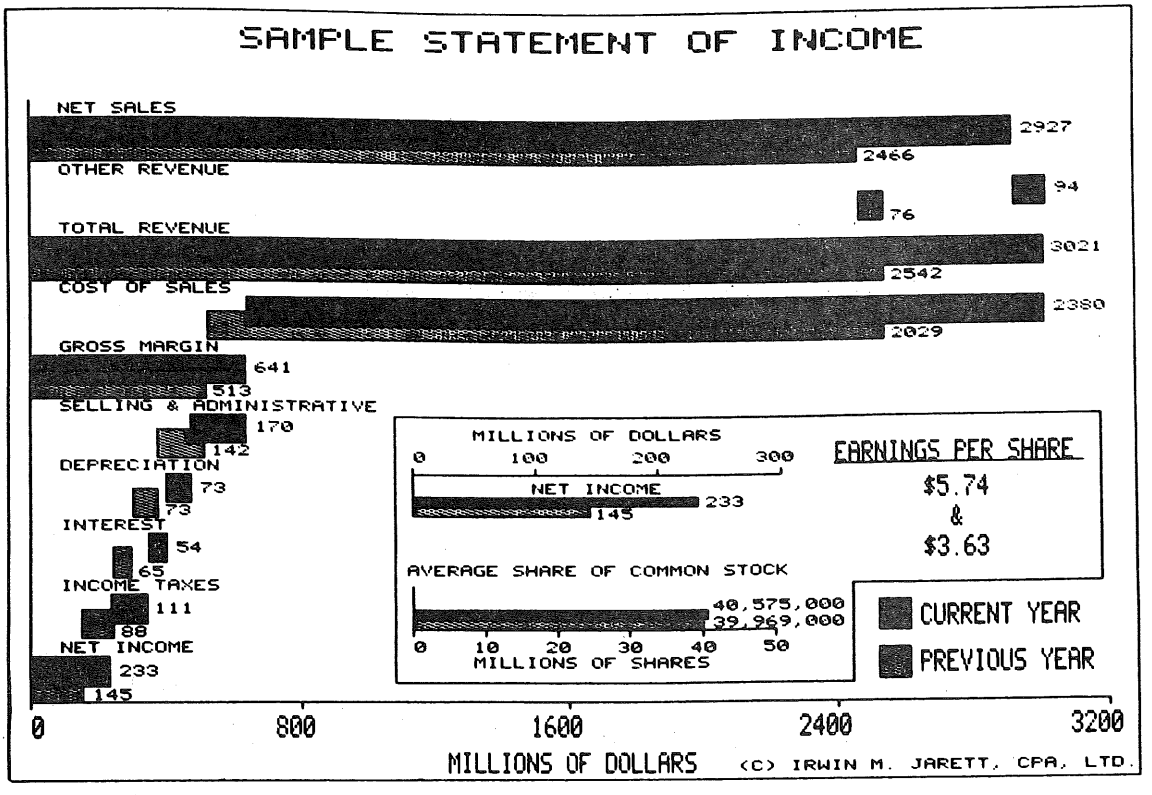
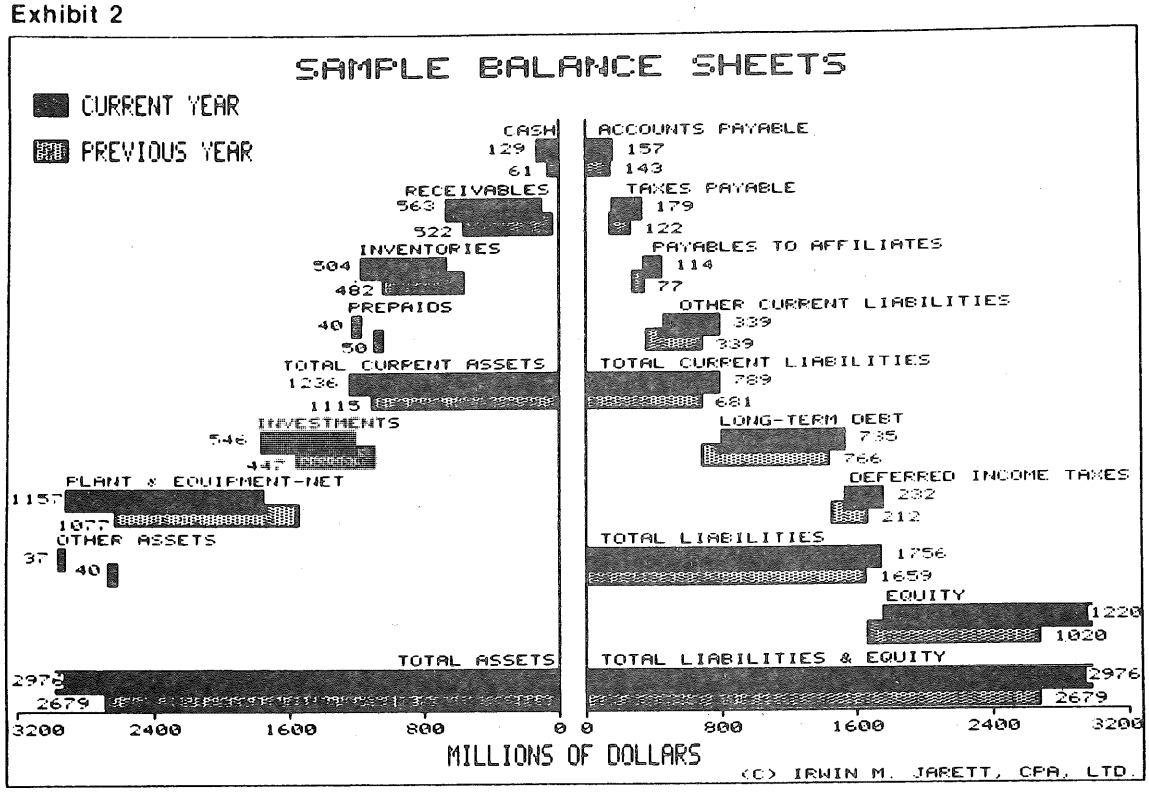


Exhibit 2



De auteur besluit zijn artikel met de volgende conclusie:

CONCLUSIONS

The tabular form of presenting financial information was dictated as much by technology as by reason. Until the development of the new graphic technology, charts and graphs were simply too costly to use as a primary means of presenting financial data. Therefore, no major effort was expended to design such a reporting format. Now, however, full-color charts and graphic presentations - with the same amount of data (perhaps more) - can be no more costly to prepare than tabular presentations.
Based on my experiences with computer graphics, I believe that we need professional guidelines and criteria if computer graphic presentations of financial statements are to be useful. Since the technology is here, it will be used. It is therefore the responsibility of the accounting profession to ensure that the financial presentations are fair and accurate and are made in accordance with predetermined and proven standards.
Terecht stelt de schrijver dat er behoefte bestaat aan "professional guidelines and criteria". Hoe immers moeten de bijgevoegde voorbeelden getoetst worden op de mate waarin ze een getrouw beeld geven van de grootte en de samenstelling van het vermogen en het behaalde resultaat? Een beleidsbepaling lijkt te eniger tijd noodzaak.

Assuring Quality Quality Assurance — Stephen L. Stamm

Datamation, March 1981
AC-documentatie O 337,

Trefwoorden: A 20, A 45; B 53

In dit artikel geeft de schrijver een wat afwijkende visie op de aanpak van de kwaliteitscontrole op applicatie software ontwikkeling. Zijn uitgangspunt luidt:
"Maak kwaliteitscontrole tot een onderdeel van ieders taak." Daarbij wordt het standpunt de kwaliteitscontrole op te dragen aan een afzonderlijke controlegroep verworpen.

Het doel van de kwaliteitsbewaking is te waarborgen dat ontwikkelde toepassingssystemen optimaal aan de gebruikerseisen voldoen en bovendien betrouwbaar, goed te onderhouden en gemakkelijk te testen zijn.

Het wordt niet realistisch geacht de uitvoering van deze taak op te dragen aan een specifieke groep:
- omdat deze voor zijn taak niet voldoende bezet kan worden. (Personen met een toereikend kennisnivo ambiëren deze functie niet als loopbaan.)
- omdat deze groep als "vijand" van de ontwerpers wordt gezien.

Meer succes ten opzichte van het voorgaande wordt verwacht als "quality assurance" in de ontwerporganisatie zelve gebracht wordt als een wezenlijk onderdeel daarvan.

Dit wil overigens niet zeggen dat er geen "quality assurance groep" zou zijn. Integendeel. Doch deze taak is "beperkt" tot de definitie van een plan (samenstel van quality assurance taken) en het toezicht op de naleving ervan als lid van het ontwerpteam.
(Zie blz. 61.)

COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.

THE PROJECT ORGANIZATIONS' ROLES IN THE SOFTWARE QUALITY ASSURANCE PROGRAM

DEVELOPMENT CYCLE PHASE	PROJECT ORGANIZATION				
	SYSTEM ENGINEERING	SOFTWARE DEVELOPMENT	TEST AND INTEGRATION	PROJECT MANAGEMENT	QUALITY ASSURANCE
Requirements Definition	• Requirements traceability • Technical review of specs	• Prepare Programming Standard Document (PSD) • Develop/implement Programmer Training Plan			• Prepare Project SCA Plan • Audit traceability analysis accomplishment • Audit spec review accomplishment • Review spec compliance to documentation stds. • Review PSD scope for completeness • Review training plan for scope • Audit training attendance
	• Prepare SW Rqt's Rev. (SRR)			• Conduct SRR • Prepare Configuration Management Plan (CMP)	• Assure SRR action item closure • Assure proper participation • Review for compliance with SQA plan
Preliminary Design	• Requirements traceability analysis • Technical review of specs and Interface Control Documents (ICD)				• Audit traceability analysis accomplishment • Audit spec and ICD review accomplishment • Review compliance to documentation standards
		• Complete PSD		• Establish engineering review/ change control board	• Review PSD for completion • Audit implementation of board
		• Initiate SW Development Folders (SDF)	• Trace test requirements to test plans		• Audit existence/completeness of SDFs • Audit traceability analysis accomplishment
	• Technical Review of PDR material	• Prepare Prelim. Design Review (PDR)		• Conduct PDR	• Assure PDR action item closure
Detail Design and Code	• Technical review of specs and ICDs	• Trace requirements to design implementation			• Audit traceability analysis accomplishment • Audit spec and ICD review accomplishment • Review compliance to documentation standards
	• Technical review of test plans	• Conduct structured walk-throughs			• Audit walk-through accomplishment • Audit Test Plan review accomplishment
	• Tech. Rev. of CDR Mat'l	• Prepare Critical Design Review (CDR) • Maintain SDFs		• Conduct CDR	• Assure CDR action item closure • Audit SDF's maintenance
Test and Operations			• Trace test plans to test procedures • Conduct test readiness meetings		• Audit traceability analysis accomplishment • Audit meeting accomplishment and procedures
	• Technical review of test procedures	• Technical review of test procedures			• Audit test proc review accomplishment • Review compliance to documentation stds.
		• Prepare DRs	• Conduct post-test meetings	• Prepare preship audit	• Certify test results and reports • Conduct preship audit
	• Prepare Discrepancy Reports (DR)		• Prepare DRs	• ERB/CCB DR disposition	• Monitor/expedite DR closure • Prepare statistical report on DR activity

Automatisering
Beveiliging
Controle
NIEUWS

door J.F.C. van Epen en drs. H.C. Kocks

Automatisering

Nieuwe technieken behoeven aandacht. Intermediair vestigt de aandacht op de glasvezeltechniek met de kop

Zand in de computer

Glasvezels gaan koperdraad vervangen

Het betreffende artikel uit de editie van 28 augustus 1981 is te omvangrijk voor volledige reproduktie. Enkele citaten mogen de sluier rond dit mysterieuze medium oplichten.

Omdat koper een schaars artikel dreigt te worden en koperdraad dus duur, zoekt de computerindustrie naar een substituut. Een bijkomende stimulans is het gegeven dat de prestaties van koperdraad de maximale mogelijkheden die de chips ons te bieden hebben enigszins teniet doen. Het substituut blijkt te liggen in optische communicatiesystemen: zand is hier de grondstof en nauwelijks schaars te noemen, bovendien overal delfbaar. Datatransport via glasvezel dus.

GLASVEZEL ALS LICHTGELEIDER

Zoals een koperdraad een elektrische stroom geleidt, zo kan een glasvezel een lichtbundel geleiden. Evenals koperdraad mag glasvezel in bochten worden gelegd, omhoog of omlaag gaan of om een spoel worden gewonden. Voor de lichtbundel is de vezel een tunnel waaruit zij niet kan ontsnappen, behalve aan het einde.
En glasvezel heeft een aantal voordelen boven koperdraad: de betrouwbaarheid is hoger, de energieverliezen zijn lager, de lichtbundel in de vezel is ongevoelig voor elektromagnetische storingsvelden.

HOE GELEIDT EEN GLASVEZEL LICHT?

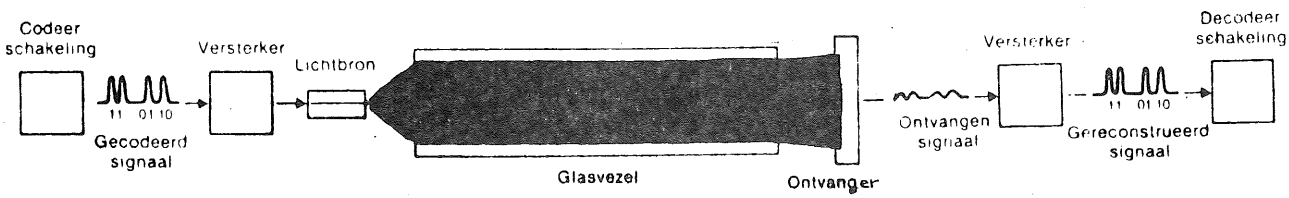
Het principe van lichtgeleiding in een glasvezel berust op de reflectie door een grensvlak dat wordt gevormd door lagen glas met verschillende brekingsindex.
De eenvoudigste glasvezel bestaat uit twee 'glascylinders'. Een kern met een bepaalde brekingsindex, en daaromheen een mantel die een lagere brekingsindex heeft.

OPTISCHE COMMUNICATIE

Bij optische communicatie wordt een lichtbundel als draaggolf gebruikt. Het signaal dat we aan de bundel willen meegeven kan analoog of digitaal zijn.

Een analoog signaal wordt via een versterker direct omgezet in overeenkomstige variaties van de lichtsterkte. De glasvezel geleidt de bundel naar een ontvanger die de variaties in lichtsterkte weer omzet in het oorspronkelijke analoge signaal. Bij het transport treedt echter lichtverlies op door absorptie en over grotere afstanden wordt het signaal te veel vervormd.
Door de analoge signalen eerst digitaal te coderen kunnen we deze bezwaren grotendeels ondervangen (figuur 1).
De lichtbron zendt nu alleen lichtflitsen uit van voldoende intensiteit. Deze pulsen representeren een code van enen en nullen, een bitpatroon. Een één is een lichtpuls, een nul het ontbreken van zo'n puls. Ook die wordt tijdens het transport verzwakt en vervormd, maar de ontvanger behoeft nu alleen het pulskarakter te onderkennen, zonder dat de exacte waarde van de lichtsterkte een betekenis heeft voor het decoderen van het signaal. Zoals het ook gemakkelijker is om te zeggen of iets rood of niet-rood is dan om de duizenden kleuren die we kunnen onderscheiden, ook alle te benoemen.
In het geval van datacommunicatie voor computertoepassingen hebben de signalen al de vereiste digitale vorm.

Figuur 1.



LICHTBRON EN DETECTOR

Aan de lichtbron van een optisch communicatiesysteem worden nogal wat eisen gesteld. De glasvezel heeft een kleine doorsnede met een beperkte acceptatiehoek - alleen het licht dat binnen een bepaalde hoek binnentreedt, wordt gereflecteerd. Door absorptie, verstrooiing en kleurbreking gaat eveneens een deel van het signaal verloren. Deze verliezen zijn tot een minimum terug te brengen door licht te nemen met een golflengte in de buurt van het infrarood en het spectrum zo klein mogelijk te houden. Verder is de gevoeligheid van de detector - aan de ontvangstzijde - bepalend voor de minimale hoeveelheid licht die de bron moet uitzenden, nadat rekening is gehouden met bovenstaande beperkingen. Fysiek moet de lichtbron ook nog passen bij de overige componenten. De koppeling met de glasvezel is bepaald geen gemakkelijk op te lossen probleem.
Tenslotte dient de lichtbron met een zeer hoge frequentie aan/uit te kunnen worden geschakeld om een grote bandbreedte te realiseren. Hoe meer bits we per tijdseenheid kunnen verzenden hoe beter.
Als lichtbronnen komen op dit moment alleen een GaAs-Laserdiode (Gallium arsenide) en een GaAs-LED (Light Emitting Diode) in aanmerking.

Beide zenden licht uit met een golflengte in de buurt van het infrarood.
De detector moet niet alleen gevoelig zijn voor kleine pulsen, maar ook een korte responsietijd hebben om in de pas te kunnen lopen met de zendfrequentie van de lichtbron. Anders zou de detector als een deler gaan werken en bij voorbeeld voor elke twee uitgezonden pulsen er één op zijn uitgang geven. Andere eisen zijn zo weinig mogelijk toevoeging van ruis aan het signaal, een zeer hoge betrouwbaarheid, passende afmetingen in relatie tot de glasvezel, lange levensduur en een lage prijs.
Op grond van al die eisen is een lawine-fotodiode de aangewezen detector. Een fotodiode kan een lichtsignaal omzetten in een elektrisch stroompje. De lawine-fotodiode heeft het grote voordeel van interne versterking. In vergelijking met een gewone fotodiode geeft een lawine-fotodiode bij dezelfde lichtpuls een grotere stroom.

WAAROM AL DIE MOEITE?

Waarom al die moeite, inspanning en onderzoek naar een nieuw communicatiemedium, dat de zaak ook nog complexer maakt? Complexer in deze zin, dat elektrische signalen omgezet moeten worden in lichtpulsen en die weer terug in elektrische signalen.
De voordelen van glasvezel ten opzichte van koperdraad zijn al even genoemd maar een tamelijk volledig antwoord op de vraag is, dat een complex van factoren er een rol bij speelt. Koperdraad wordt duur en de kabels gaan een steeds hogere kostenpost vormen in computers. Verder weegt het draad nogal iets en nemen de kabels veel ruimte in.

Het essentiële knelpunt is echter dat koperdraadverbindingen de prestaties van de moderne computers - zeker die van de komende generaties - verlagen ofwel drukken tot een peil dat beneden het maximum ligt van de chips.
Tussen de zeer hoge verwerkingssnelheden van de chips en de maximaal mogelijke doorvoercapaciteit van koperdraad dreigt een discrepantie te ontstaan. De chips kunnen per seconde meer bits ontvangen en verwerken dan de koperdraad kan aanleveren. En omgekeerd leveren de chips meer uitvoer - in de vorm van bits - dan de koperdraad kan transporteren. Kortweg: de bandbreedte wordt te klein.
Een ander probleem dat daar nauw mee samenhangt komt voort uit de toenemende integratie van de circuits. De circuits op een chip zitten niet alleen zo dicht op elkaar gepakt om ruimte uit te sparen, maar ook om de verbindingen zo kort mogelijk te houden. Hoe korter de verbindingen hoe sneller het circuit kan schakelen. Kortere verbindingen vormen één factor om de snelheid te verhogen, de andere is schakelen met kleinere spanningsverschillen.
Een circuit wordt gestuurd met spanningssprongen of pulsen die al naar de gehanteerde logica de betekenis van een nul of een één hebben. Hoe kleiner nu het spanningsverschil waarvoor het circuit gevoelig is, hoe sneller het werkt. Met als voordeel bovendien dat minder energie nodig is en verloren gaat in de vorm van warmte.

Die noodzakelijke eis van een zeer kleine spanningssprong schept een probleem. Hoe kleiner de puls, hoe stabieler de aardleiding - van koper - moet zijn.
Om een idee te geven. TTL-circuits (Transistor to Transistor Logic) werken op pulsen van 5V. Of de aardleiding dan exact nul is, maakt niet veel uit. Ook een puls van ongeveer 0,8V voor ECL-circuits (Emitter Coupled Logic) is nog gemakkelijk te onderscheiden.
Voor CML-circuits (Current Mode Logic) is het signaal maar 4 millivolt en dan is het wel een heel probleem om de aardelijn stabiel op nul te houden. Ook de lengte van de kabel waarover de puls loopt, kan een kink in de kabel veroorzaken door zijn weerstand.

Glasvezel vormt om al deze redenen een even noodzakelijk als goed alternatief: een hogere bandbreedte (theoretisch tot in tientallen Gbits/s), geen problemen met een stabiele aarde, ongevoelig voor elektromagnetische storingsvelden, geen problemen met potentiaalverschillen over de lengte, maar wel een veel hogere betrouwbaarheid. Waar het geringere gewicht, minder ruimtebeslag en een bijzonder goedkope grondstof, waaraan nauwelijks gebrek is, nog aan kunnen worden toegevoegd. Heeft men de massaproduktie en technologie eenmaal onder de knie, dan kunnen de kosten aanzienlijk dalen.

DE HUIDIGE STAND VAN ZAKEN

Op dit moment zijn voor toepassingen met een transmissiecapaciteit of bandbreedte van 20 tot 50 Mbits al een grote verscheidenheid aan optische verbindingen beschikbaar. Wat betreft de koppeling van bijv. snelle schijfgeheugens aan een computer met glasvezel, is er geen enkel probleem, gezien de vereiste bandbreedte van 2 Mbits/s.
J.P. Lazzarri verwacht dat rond 1985 optische verbindingen in produktie kunnen worden genomen voor de koppeling van randeenheden met computers.
De research is nu vooral gericht op een bandbreedte van 200-400 Mbits/s om het mogelijk te maken de verschillende eenheden in een computersysteem met glasvezels te verbinden. Te denken valt aan de verbinding tussen hoofdgeheugens en de computerlogica voor de interne besturing, de logische en de rekenkundige bewerkingen. Deze logica bevindt zich in een eenheid die ALU (Arithmetic Logic Unit) wordt genoemd.
Maar dat zal volgens een schatting van J.P. Lazzari, pas in 1988 het geval zijn.

IS DE GLASCOMPUTER EEN REËLE MOGELIJKHEID?

Op grond van het bovenstaande kunnen we een beeld schetsen dat er voor, laten we zeggen 1990, ongeveer als volgt uitziet.
Randapparatuur (terminals, magneetband- en schijfgeheugens) werken volgens elektromagnetische principes. De bits die zij aanbieden in de vorm van kleine stroompjes worden door lasers omgezet in lichtpulsen.

Deze gaan via glasvezels de computer in, en worden vervolgens weer omgezet in stroompjes of spanningen voor de vastlegging in geheugenchips. De verbinding tussen deze chips en de chips van de ALU bestaat dan weer uit glasvezels. Intern vindt die hele omzetting dan nog een keer plaats. Op zich hoeft dat geen probleem te zijn gezien de hoge snelheid, bandbreedte en betrouwbaarheid (momenteel al in de orde van 10^{-10}, één fout op de 10 miljard bits).
Toch ligt het voor de hand om je dan af te vragen of de geheugens niet geheel in een optische technologie zijn uit te voeren en wellicht in een wat later stadium ook de computerlogica in de ALU.

DE HUIDIGE TECHNOLOGIE ALS BARRIÈRE

De bestaande technologie voor de gegevensvastlegging met zijn veelbelovende perspectieven vormt een krachtige barrière om te beginnen aan een heel nieuwe techniek. Een soortgelijke barrière is er ook wat betreft de chips. De miniaturisering is nog lang niet ten einde en de investeringen moeten eerst worden terugverdiend.
In zekere zin ligt de zaak andersom: de voortgaande ontwikkelingen binnen de bestaande technologie zijn gestuit op de beperkingen van het koperdraad. Door glasvezels toe te passen voor het gegevenstransport tussen de verschillende eenheden wordt juist een barrière voor de verdere ontwikkeling van de bestaande technologie opgeruimd en komt deze nog steviger in het zadel te zitten.

Kleinschaligheid blijkt opnieuw succesformule

Onder deze kop geeft de Automatisering Gids in zijn editie van 23 september 1981 een nabeschouwing van de beurs Computer '81 die in de Rotterdamse Ahoy' Hallen werd gehouden in de derde week van september. Uit dit artikel laten wij enkele passages volgen.

Na Tekst '81 en Europe Software heeft vorige week de derde automatiseringsmanifestatie Computer '81 bewezen bestaansrecht te hebben. De kleinschaligheid slaat toe in de computerbranche. Geboren uit onvrede over een mammoettentoonstelling als de Efficiency Beurs, uit rebellie tegen de gevestigde orde van de Vifka, uit veranderde commerciële opvattingen over marktbenadering, of uit wat voor andere edele of minder edele overweging dan ook, de kleine beurs is in.

Vorige week vonden ruim twintigduizend bezoekers hun weg naar de 8.000 m2 tentoonstellingsruimte die in de Rotterdamse Ahoy'-hallen voor Computer '81 waren gereserveerd. Dat waren er meer dan aanvankelijk was verwacht en ook de kwaliteit van het bezoek gaf reden tot tevredenheid. Een voortzetting dus van de trend die al bij Tekst '81 en Europe Software is ingezet. Een eenduidige verklaring voor het succes van de kleinschaligheid is niet te geven, maar er zijn wel enkele

factoren die ongetwijfeld een rol spelen op te noemen. Een van de factoren is dat de systemen (met name de hardware) goedkoper worden en ook beter aangepast aan kleinere organisatie-structuren.
Juist voor die kleine organisaties is het in de zware economische tijden bittere noodzaak veel aandacht te besteden aan het opvoeren van de efficiency en dus om te overwegen of de toepassing van een computer daarvoor zinvol is. Dit naar elkaar toe groeien van vraag- en aanbodzijde van de markt is een ontwikkeling die zich de laatste jaren nadrukkelijker dan voorheen heeft doen gelden. Een factor die daar nauw mee samenhangt is het feit dat het bij een toename van het aantal potentiële computergebruikers commercieel aantrekkelijk wordt de 'bewerking' van de markt regionaal aan te pakken.
Door Computer '81 is bevestigd wat al door het succes van de Grafivak bleek: ook voor initiatieven van buiten de branche blijkt er een voedingsbodem te bestaan. Het publiek bij Computer '81 was echter niet uitsluitend afkomstig uit de regio Rotterdam. De doelgerichte aanpak bij de beurs gericht op het tonen van computers en wat daar zeer nauw mee samenhangt spreekt voldoende aan om mensen uit heel Nederland en zelfs van daarbuiten aan te trekken.

CONGRES

Het aan Computer '81 gewijde congres mocht zich ook in een goede belangstelling verheugen. De benadering van gebruikersstandpunt uit sloeg aan. De reklamepraat van leveranciergebonden sprekers bleef achterwege om de doodeenvoudige reden dat er nauwelijks van leveranciergebondenheid sprake was. Organisator Hirdes Advies was er in geslaagd sprekers te vinden die geacht mochten worden wat objectiever te zijn. Het congresbezoek bleek overigens net als het beursbezoek lang niet zo gemakkelijk te overdonderen als gevreesd had mogen worden. Het publiek was kritisch. Een van de sprekers die daarover kan meepraten is drs. Terpstra, beleidsmedewerker van het Ministerie van Economische Zaken. Na een uiteenzetting van zijn zeer recente subsidieregeling bereikte hem uit het publiek een aantal zeer kritische vragen. Men vroeg zich bijvoorbeeld af hoe men het tijdsverschil tussen goedkeuring van een voorstudie naar automatisering bij een bepaald bedrijf en de uitvoering van een project, dat voordat een opdracht wordt verleend ook eerst in essentie door een commissie van vijf bij het ministerie moet worden goedgekeurd, kan overbruggen.
Moet, zo vroeg men terecht, het project dan 45 à 90 dagen stilliggen met alle risico's die daaraan verbonden zijn?

EINDELIJK IS HET DAN ZOVER. OOK .....

IBM komt met micro

Al geruime tijd werd er gespeculeerd over het feit, dat IBM de markt van personal computers op zou gaan. Aan alle geruchten dienaangaande is nu een einde gekomen, IBM heeft het inderdaad gedaan.
Begin deze maand annonceerde het bedrijf haar 16-bits microcomputer. Het hart van de micro wordt gevormd door de Intel 8088 microprocessor.

Het apparaat wordt voor het grootste gedeelte vervaardigd in IBM-vestigingen in de VS en Canada. Alleen het beeldscherm en de printer komen uit het Verre Oosten, te weten respectievelijk uit Taiwan en Japan.
In de minimale configuratie beschikt de persoonlijke micro van IBM over 16 kilobytes geheugen. Het interne geheugen is uitbreidbaar tot een maximum van 256 K. Naast deze 16K RAM heeft de basisconfiguratie ook nog eens 40K ROM aan boord. Gebruik kan worden gemaakt van het eerder genoemde beeldscherm, maar de micro van IBM kan ook worden aangesloten op een kleuren- of zwart/wit TV.
Het apparaat heeft een karakterset van 256 karakters, die in 8 voorgrond- en met 8 achtergrondkleuren kunnen worden afgebeeld. Grafische karakters kunnen in 4 verschillende kleuren afgebeeld worden. De prijs van de IBM micro varieert van 1.565 dollar voor het basissysteem tot ruim 5.000 dollar voor de meest uitgebreide uitvoering. De IBM micro kan worden geprogrammeerd in twee talen, namelijk Basic en Pascal. Geheel in de lijn van IBM is er veel aandacht besteed aan de software. Wat de systeemsoftware aangaat, kan men kiezen uit drie verschillende operating systemen. De eerste draagt de naam 'DOS', een ontwikkeling van Microsoft. Tweede mogelijkheid is CP/M-86, het welbekende DOS voor 16-bitters van de Amerikaanse firma Digital ch. Als derde kan gekozen worden voor het UCSD P-systeem, een systeem met uitgebreide mogelijkheden voor Pascal.
Ook heeft IBM bekende applicatieprogramma's geschikt gemaakt voor haar persoonlijke micro. Vermeldenswaard zijn Visicalc, het rekenprogramma van Personal Software, en de Easywriter tekstverwerkingssoftware van de firma Information Unlimited Software.
De introductie van deze personal computer luidt voor IBM een geheel nieuw tijdperk in. Zo is dit het eerste computersysteem, waarvoor IBM niet zelf de systeemsoftware heeft ontwikkeld. De persoonlijke micro is tevens het eerst IBM-systeem, dat niet uitsluitend is bedoeld voor een zakelijke gebruikersomgeving.
De nieuwe micro zal in oktober van dit jaar op de Amerikaanse markt komen. Het is nog niet bekend, wanneer de nieuwe micro in Europa c.q. Nederland verkrijgbaar zal zijn. Buiten Nederland zal de verkoop waarschijnlijk kunnen verlopen via de enkele vestigingen van Computerland.

Beveiliging

In het meinummer 1980 van het tijdschrift Information Privacy analyseert Kenneth Wong een aantal aspecten met betrekking tot computerbeveiliging en privacy in het Verenigd Koninkrijk. Hij doet dit naar aanleiding van onderzoeksresultaten omtrent verwachtingen in de tachtiger jaren die er bij de ondernemingen leven.
Hij gaat onder meer in op preventieve maatregelen tegen stakingen e.d. Door bijvoorbeeld alleen op de computerafdeling te laten staken kunnen vakbonden de ondernemingen grote schade toebrengen.
Wij citeren enkele alinea's uit het artikel van Kenneth Wong.

INDUSTRIAL ACTION

101 cases of industrial disputes involving computer installations have been recorded in the UK, most of which resulted in some form of industrial action against employers. This included walkouts, overtime bans, refusal to work with new computer equipment, noncooperation, and total withdrawal of labour. Many caused serious disruption to business operations and inflicted heavy losses on organizations through cash flow delays, loss of new business, and turning existing customers away to business rivals.
The British Post Office (BPO) and UK Civil Service disputes in 1979 saw further sophistication in strike strategy, with large trade unions involving only a small number of key computer staff in actions that resulted in total disruption of cash flow and services. Strike funds were levied from the rest of the union members involved in the disputes. As the strikes were prolonged, the BPO ran into serious cash flow problems and the affected areas in government machinery were totally paralysed. Yet the strikers suffered little, if any, loss in earnings.

Kan een rekencentrum zich hierop voorbereiden? Kenneth Wong:

The UK Confederation of British Industry is investigating the introduction of antistrike insurance to provide some financial compensation to companies suffering from serious disruptions in production and loss of profits through strikes. There have been repeated press reports of possible amendments to industrial relations legislation to outlaw secondary picketing and closed shop working *.
Social welfare benefits to strikers families could be stopped and replaced by a loan system instead. However, it could take a considerable time to finalise these measures. Their subsequent implementation could also spark off a series of protest disputes from militant unions.

---

* Secondary picketing refers to industrial action against an employer not directly involved in the dispute. A closed shop refers to mandatory 100% union membership.

In this developing scene it is crucial that DP management brief their general management clearly on the scale of potential disruption.

Vervolgens komt een aantal meer bekende oorzaken van schade aan de orde, waarvan wij ook enkele citaten laten volgen.

COMPUTER DISASTERS

When a computer installation is seriously damaged by fire, flood or explosion, recovery can take months to complete. This is exemplified by a recovery timescale drawn up by a major insurance company using computer applications in batch mode. For online systems, the disruption is more devastating.
Many cases of flooding or water damage due to burst pipes happened during winter 1979, causing hundreds of thousands of pounds of damage to computer equipment in each case. If future winters are as bad, similar incidents of water damage could be repeated.
The most devastating disasters to computer installations are those of fire and explosion. Figure 1 shows a typical recovery timescale.

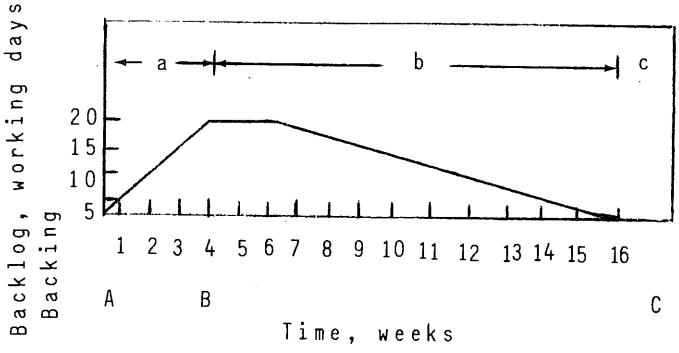


Figure 1. Typical recovery timescale (A-incident, B-resumption of data processing, C-resumption of normal DP working, a-downtime, b-DP recovery time, c-continuing clerical recovery).

There have been many cases of minor fires that were detected quickly and put out promptly, causing little damage to the installation. Others were allowed to develop and spread and caused extensive damage to property.

COMPUTER ABUSE

Information on 30 cases of computer fraud and theft in the UK has been collected. Figure 2 illustrates that most cases incurred losses of less than £ 10.000. Several cases were also reported where the losses were in excess of £ 100.000 each. In the USA, SRI have reported over 400 cases of computer abuse, some of which involve wilful damage to property and equipment, while others were perpetrated for financial gains.
Average loss per case in the USA was approximately £ 850.000.

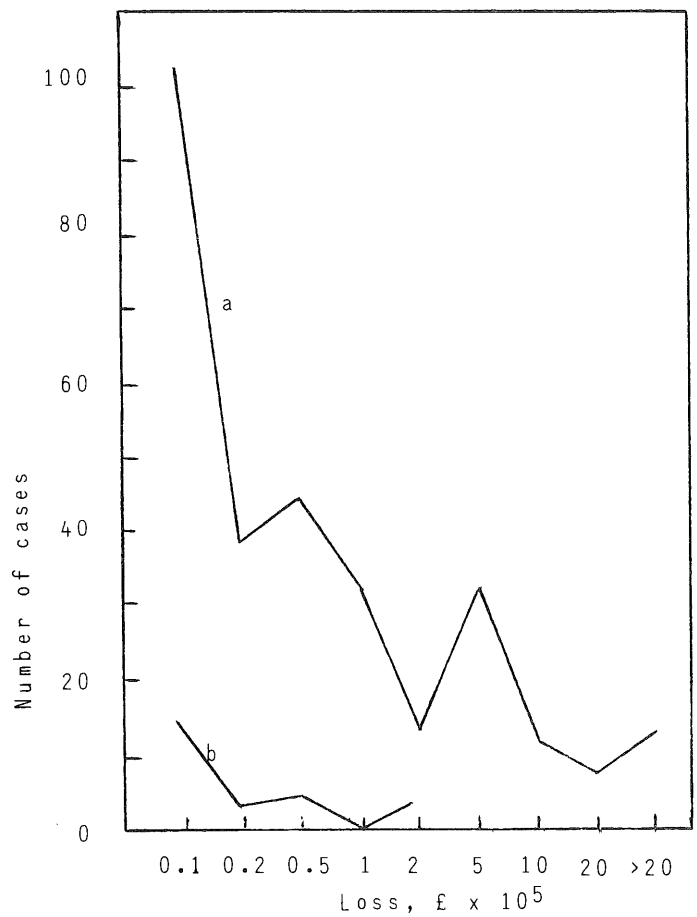


Figure 2. Computer abuse in the USA and computer fraud and theft in the UK (a-USA, b-UK): average loss = £ 850.000 in the USA.

OTHER ISSUES

Several major developments are likely to affect the security of computer systems in the 1980s. Designers of large operating systems have given serious consideration to the prevention of access violation

from computer users, as exemplified by IBMs MVS. These are likely to deter potential prepetrators scheming for private gain through illegal modification or manipulation of financial data in computer systems. Better standalone access control proprietory software has also emerged in the marketplace to provide further protection. The recent growth of microprocessor technology would encourage the cheap production of cryptographic chips in data communications to protect against wire tapping of communication lines. Microprocessors will also encourage the development of sophisticated physical access control systems with built in memory to record staff movement, to guard premises and installations.
Microprocessor technology will also significantly help the market growth of personal computers. As the public gets more accustomed to personal computing, the number of potential electronic criminals is likely to increase, making it difficult for installations to guard against illegal coding built in applications programs. To counter this threat, the use of high level languages will be further promoted for application programming.

Door de introductie van privacy-wetten kan het noodzakelijk zijn de geautomatiseerde systemen zoals die van het internationaal betalingsverkeer aan te passen. Indien dit niet adequaat en niet tijdig gebeurt kan dit storingen in de computerverwerking ten gevolge hebben.

COMPUTER PRIVACY

Transborder dataflow between UK and countries with existing privacy legislation could be seriously obstructed through data-protection authorities if the latter forbids such traffic with installations located in countries with relaxed privacy rules. This was evidenced by several instances of UK firms losing contracts as a result of restrictions imposed by the Swedish Data Inspection Board on the handling of personal data, such as mailing lists, in countries that have not enacted data-protection safeguards equivalent to those in force in Sweden. The argument extends further to multinational companies transferring data from one installation to another located in a different country.
The implementation of the Data Protection Act in the UK will require employers to provide proper safeguards to enforce physical access control into computer installations, as well as proper access control procedures to gain access to personal data. As a result the general security of computer installations would be tightened. In future, privacy safeguards could be a major contributing cost in the development of new information systems.
More attention would be paid to the setting up of audit trails to trace the flow of information as well as to facilitate the early detection of access violation and data corruption.

CONCLUSION

Problems of industrial action, disaster, abuse and privacy legislation will continue to beset company executives charged with the responsibility of computer security. New technology will offer assistance to the defender in some cases and the potential perpetrator in others. The future is full of 'ifs' and 'buts'. It is necessary to plan ahead, in anticipation of new hazards and new legislation. Proper provision should be made of safeguards to reduce the likelihood of the occurrence of hazards and to lessen the impact of laws when they are introduced.
The importance of security and privacy issues in computer systems will increase during the 1980s for the following reasons:

- a greater reliance on computers as they applied more widely;
- increasing social unrest;
- newer database and network technologies.

Advances in technology are improving hardware reliability, so that the shift in emphasis in the 1980s will be towards protection against saboteurs and disasters, such as fires.

Het onderwerp "beveiliging" kan zich verheugen op een brede belangstelling. Dit was reden voor de Sectie Beveiliging van het N.G.I. om op 24 september 1981 een ledenbijeenkomst te beleggen rond het onderwerp Fysieke Beveiliging van Rekencentra. In de Automatisering Gids van 14 oktober jl. troffen wij een samenvatting aan van deze bijeenkomst. Hieruit laten wij enkele fragmenten volgen.

Nuttige tips op NGI-bijeenkomst

Beveiliging is geen eenvoudige zaak

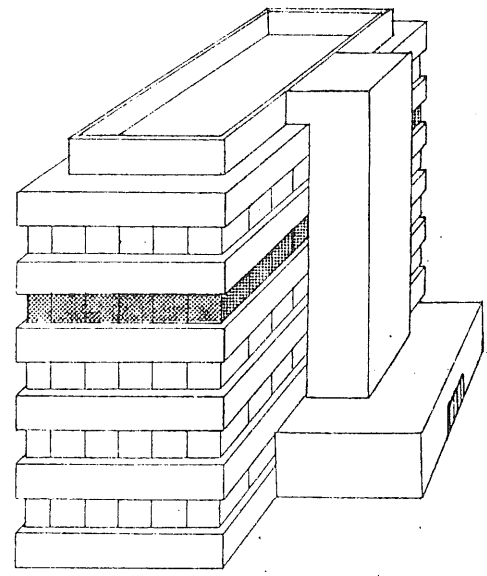
Beveiliging van computercentra is een verre van eenvoudige zaak. Er moet een afweging plaatsvinden tussen wat technisch mogelijk en sociaal haalbaar is. Dit bleek weer eens op de eerste bijeenkomst in het nieuwe seizoen van de sectie beveiliging van het NGI. Als spreker was uitgenodigd de beveiligingsadviseur W. van der Ham. Deze gaf op basis van twintig jaar praktijkervaring tal van nuttige tips.

Van der Ham begon met de vraag te stellen "wat is beveiliging?" Bij het beveiligen van een computercentrum moeten we zoeken naar een evenwicht tussen te nemen beveiligingsmaatregelen en het aanvaarden van ingecalculeerde risico's in de procesgang. Er zijn maatregelen die continu in werking zijn en maatregelen die wel reeds voorbereid zijn maar pas actief worden als de omstandigheden hiertoe aanleiding geven.

OVERLEG ARCHITECT MOEIZAAM

Belangrijk in het kader van beveiliging van nieuwbouw zijn de besprekingen met de architect. Deze zijn doorgaans moeizaam. De architect maakt meestal de fout een kantoorgebouw te ontwerpen, waarin dan een computercentrum moet komen. Aan een gebouw, c.q. ruimte, voor een computercentrum moet echter deels geheel andere eisen worden gesteld dan aan dat voor een kantoor. Van der Ham vindt dat als de computerruimte op de begane grond is gevestigd, ze vanaf de straat niet zichtbaar mag zijn. Hij geeft daarom de voorkeur aan blinde muren rond de computerruimte.
Een bezwaar dat wel wordt genoemd is dat de operators dan geen daglicht zien. Dit zou van de Arbeidsinspectie niet mogen. Daar valt echter altijd over te praten. Als er ten behoeve van de operators een kantine, c.q. recreatieruimte, wordt gerealiseerd waar wel daglicht binnenvalt, zal de arbeidsinspectie instemmen met de 'dichte' computerruimte. Het liefst ziet hij deze recreatieruimte naast de computerruimte gesitueerd.
Over hoogbouw bestaan veel strijdpunten. De kelder wordt nogal eens aangeprezen als de meest geschikte computerruimte. Een nadeel is dat een kelder onder water kan raken, bijvoorbeeld door blussingswerkzaamheden op een hogere etage. Persoonlijk geeft Van der Ham er de voorkeur aan de computerruimte te situeren op de een na hoogste etage. Mits de maximale vloerbelasting dit toestaat en de beschikbare hoogte toereikend is. Een bezwaar is dat de uitbreidingsmogelijkheden beperkt zijn. Steeds meer komt daarom 'split-level' in zwang. De niet-bediende apparatuur wordt een etage hoger of lager geplaatst.

Voordeel van de op een na hoogste etage is dat vanaf de straat de computerruimte en -apparatuur niet zichtbaar is. De toegang is bovendien goed af te sluiten. Doordat je dicht bij het dak zit, beschikt de eventuele airconditioning over een korte verbinding met de buitenlucht. Een ander belangrijk voordeel houdt verband met de luchtbehandelingsinstallatie. Van der Ham heeft het meegemaakt dat bij een computercentrum de verse luchtaanzuig zich anderhalve meter boven het trottoir bevond. Dit is "in wezen immers gevaarlijk". Als iemand kwaad in de zin heeft en bij de luchtaanvoeringang een fles zoutzuur kapot gooit gaan de metalen delen in de computer na enige dagen ernstig oxyderen.
Van der Ham wil dat door de architect bij het ontwerp van de hoogbouw daarin een opstaande rand wordt opgenomen. Het dak is immers een ideale plaats voor allerlei apparatuur zoals airconditioning, generatoren, eventueel frequentieomvormers, etc., en de opbouw voor de liftschacht. Om dit alles aan het zicht te onttrekken is een opstaande rand ideaal (zie bijgaande schets) die wij van de spreker ontvingen en derhalve niet in de Automatisering Gids is geplaatst.



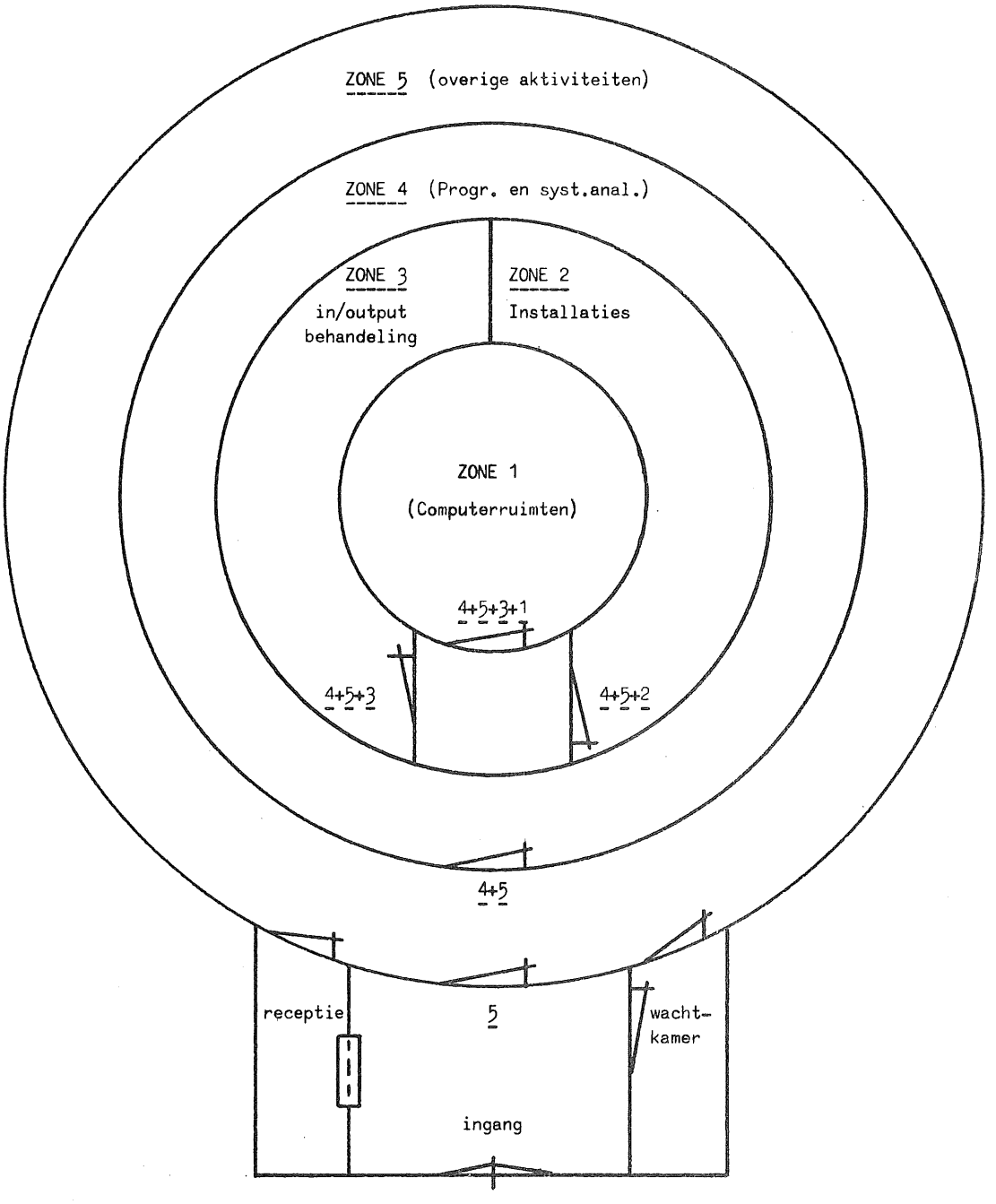
De architect wil het meestal niet. Later echter, als er al diverse apparatuur op het dak staat, gaat men veelal over tot het plaatsen van schotjes. Dat is veel minder fraai dan vooraf een opstaande rand geïntegreerd in het ontwerp op te nemen. Als er nieuwbouw wordt gepleegd is het verschrikkelijk belangrijk de beveiligingsfunctionaris al bij de bouw te betrekken. Deze kan mogelijke fouten in de lay-out of zaken die de beveiliging bemoeilijken, elimineren.
De taak van de beveiligingsfunctionaris vereist dat de man moet beschikken over goede contactuele vaardigheden.
Eigenlijk moet hij 'geliefd' zijn bij zijn collega's. Het personeel moet bovendien absoluut overtuigd zijn dat beveiligingsmaatregelen noodzakelijk zijn.
Het welslagen van de beveiligingsfunctie is afhankelijk van drie factoren, te weten bouwkundige voorzieningen plus hulpapparatuur, een goede organisatie en medewerking van de betrokkenen. De directie moet zijn volle medewerking verlenen en mogelijkheden voor beveiliging creëren. Het verdient voorkeur de toegang tot de computerruimte zelf te blokkeren voor onbevoegden. Het alleen toelaten van operators leidt tot een beter werkklimaat.

ZONE-INDELING GEWENST

Een aspect van bouwkundige voorzieningen is het creëren van zones. Er moet er minimaal één zijn, de computerruimte zelf. Bij bijvoorbeeld vijf zones is de volgende indeling mogelijk. Zone 5: overige activiteiten, 4: analisten en programmeurs, 3: input/output-behandeling, 2: installaties (operators moeten daar bijv. niet zelf kunnen schakelen. Dus afsluiten, desnoods met sleutel, als iedereen maar wegblijft die er niet hoort) en zone 1: de computer(s).

De hierna volgende schematische tekening, die wij eveneens van de heer Van der Ham ontvingen, moge een en ander verduidelijken.

Schematisch overzicht van de beveiligingszone in een computercentrum.



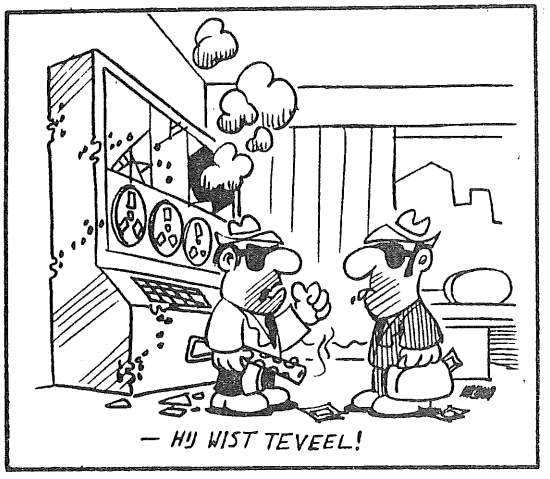
Separate toegang en receptie, toegankelijk vanuit het hoofdgebouw, of van buiten.

Bedoeling van de zone-indeling is in de eerste plaats de operators een rustige werksfeer te bezorgen. Er wordt een drempel opgeworpen zodat het niet mogelijk is dat iedereen eventjes de computerruimte binnendringt. Zowel onbevoegden, c.q. ondeskundigen, als degene met kwade bedoelingen kunnen geweerd worden.

TOEGANGSCONTROLE

Op het gebied van toegangscontrole zijn er zoveel hulpmiddelen op de markt dat je door de bomen het bos niet meer kunt zien, merkte Van der Ham op. Hij adviseerde bedenktijd te nemen na een bezoek van een vertegenwoordiger. Is het allemaal wel bruikbaar en nuttig? Voor externe beveiliging kun je bijv. een key-card introduceren. Deze zijn er ook voorzien van een foto van de drager. Maar waar is een foto goed voor? Om de drager van de key-card te herkennen? Er is geen enkele portier die de drager zal vergelijken met de man op de pasfoto. Er is geen noodzaak aanwezig voor een pasfoto en het nuttig effect is bovendien gering.
Het op de key-card vermelden van de naam van het bedrijf is alleen maar gevaarlijk. Wel kan het zinvol zijn de key-cards een kleuraanduiding te geven die correspondeert met de zone-indeling. De kleur op de key-card geeft dan aan tot welke zone de drager toegang heeft.
Nieuw als toegangshulpmiddel is een kleine nylon sleutel. Deze komt aan bepaalde bezwaren van de key-card tegemoet. Hij kan gewoon aan een sleutelring worden bevestigd, waardoor je hem minder gauw vergeet. Verder wordt beweerd dat deze sleutel zo sterk is, dat hij nooit kapot kan gaan.
Als er eenmaal beveiligingsapparatuur bij een bepaalde leverancier is besteld, zal deze als hij de kans krijgt, het installeren aan de klant over willen laten. Daar moet u als koper echter niet mee akkoord gaan. De bestelling moet als turn-key-project (in de figuurlijke en letterlijke zin van het woord) worden uitgevoerd.
Een nooddeur naar buiten is een groot gevaar voor de beveiliging. Met behulp van binnenuit is het mogelijk dat onbevoegden binnendringen. Het sluiten van een contact dat een signaal geeft als de deur open is, is onvoldoende. Momenteel zijn er echter sloten met microswitch op de markt. Eén milimeter verplaatsing van het slot geeft direct een signaal.
Tot slot ging Van der Ham in op het aspect van de energievoorziening. Het kan onacceptabel zijn als de spanning wegvalt. Niet zozeer omdat dit een achterstand in het werk oplevert. Die kan in een weekend worden ingelopen. Het abrupt wegvallen van elektriciteit kan er echter toe leiden dat de zwakke broeders onder de hardware het dan plotseling laten afweten. Dit is het gevolg van piekbelasting, die kan optreden na het wegvallen van de spanning.

Een niet te veronachtzamen onderdeel van de maatregelen ter beveiliging van de continuïteit in de computerverwerking is de zorg voor een adequate uitwijkmogelijkheid. Hier en daar ontstaan daartoe speciale uitwijkcentra. Deze kunnen bestaan uit gebouwen met alle benodigde voorzieningen, echter zonder apparatuur, dan wel uit compleet met computers uitgeruste centra. In Compact nr. 24 zomer 1981 pag. 57 wordt de oprichting van een dergelijk centrum gemeld.



Controle

In het volgende artikel - gedeeltelijk weergegeven - wordt een pleidooi gehouden voor het gebruik van grafische voorstellingen in de "accounting profession" en de noodzaak van standaarden voor het gebruik ervan. De vraag is of de argumenten die aangehaald worden ook niet van toepassing zijn op de "accountantsprofessie". Het geven van een antwoord erop wordt aan de lezer overgelaten.

CPA ADVOCATES REVOLUTION IN FIELD'S USE OF GRAPHICS

Speaking at the American Institute of Certified Public Accountants (AICPA) computer conference, Jarett advocated a revolution in the presentation of financial data. Accountants should grasp the new graphics technology, he said, because it could ultimately simplify complicated financial procedures.
There are other reasons why accountants should embrace graphics, according to Jarett.
First is the "unbearable problem" of needless paper that management has to deal with daily. He said that graphics charts could eliminate a great deal of paper, allowing an executive merely to glance at a chart. "Who's reading all of that paper anyway?" he asked.
Secondly, Jarett said that using charts in presenting data was simply a better way to do it, noting that a chief financial officer wants to get to the bottom line quickly.
The lower cost of graphics equipment presently available is a third reason for the revolution, according to the speaker.

Standard Needed

Jarett urged attendees to make the accounting profession aware of the need for computer graphics and especially the need for a set of standards. "The ability to produce graphics has sprung upon us", he said, adding that presentation of information and reduction of paperwork are the two chief benefits of graphics systems.
The major stumbling block is that there has been virtually no research done in financial graphics, Jarett said. He conceded that there are many vendors that offer graphics systems, but noted that they do not supply anything for the financial community.
The speaker offered a major computer vendor's annual report as an example of the power of graphics in the financial world. Looking through the report, he noticed that the company's profits were presented in red. It is common knowledge that when a company is "in the red", it is not profitable. Profits are traditionally shown in black. This type of misrepresentation could be dangerous, Jarett indicated, mentioning that the company's executive did not even realize the negative appearance.

Jarett said that the whole arena of colors is an extremely important part of graphics, especially in accounting. He suggested that computer-generated graphics for the accounting profession be developed in black and white to avoid potentially hazardous situations. "Accountants show a lot of data. Graphics is no toy. You can make people change their behavior by using graphics", he said.
Five types of comparisons are normally done in graphic charting, according to the speaker. The correlationship type is the most important to accountants because it shows current liabilities and assets. He showed examples of different graphics representations and noted that the human brain will pick up on certain patterns and make decisions without needing to know written data.
The manner in which financial graphs are presented is crucial to accountants because they can be held legally responsible for the way the data is perceived. "The pattern ability of the brain is unbelievable. It can compare industries, countries and currency by graphics representation", Jarett said.
This need for accuracy necessitates standards for accounting graphics noted the speaker. "We're the ones to set standards. We don't want a graphics artist to present financial statements", he added.
Jarett said that he was not getting much help from the National Computer Graphics Association or from vendors when asked about assistance. He did say, however, that there is currently a major study being done at the University of Texas in this field, and there is a software model being tested at Harvard University.
It is, he concluded, the accounting profession's responsibility to push for financial graphics, and if they do not, they may fall behind for the technology.

Computerworld, 1.6.1981

NEW WORLD OF CORPORATE DP AUDITORS SIGHTED

- A brave new world of DP professional is emerging from the corporate world - the DP auditor.

Aldus de inleiding van een artikel in Computerworld nr. 20 van 18 mei 1981, geschreven naar aanleiding van de eerste Information Systems Control Conference. Een vijfdaagse conferentie, gesponsored door het Institute of Internal Auditors (IIA), gericht op de noodzaak voor "professional auditors" om zich op het gebied van data processing te scholen.

Because auditing in the past was primarily a manual procedure, the acceptance of the computer and internal control software has not come easily to "green visor" auditors. This resistance, coupled with the feeling among DPers that auditors represent a threat, has often produced bad feelings, officials said. These feelings are compounded because auditors are sometimes reluctant to ask important systems questions, but "the brave ones are learning the new technology".

"An adversary type of effort resulted in a lot of companies because of these confrontations between DP people and auditing staffs", noted Lee Haynes, conference chairman. He referred to a study of internal controls in U.S. corporations conducted by the Graduate School of Business Administration at the University of Michigan which showed the extent of the conflict between these two groups.
Auditing department managers now realize that their auditors need DP training if they are to perform their jobs efficiently, Haynes said. The extent of that training should depend upon the level of auditing personnel in the corporation.
The first level includes the general auditor. He should have some knowledge of the DP function and how it might help in managing corporate resources, Haynes said.
The second level includes the auditing director or manager. This person should have more systems knowledge than he does now, Haynes indicated.
The DP auditor is the third level. This person is chiefly responsible for auditing information systems. Haynes' big concern here is that many times an auditor audits "around the computer" by asking people what's going on rather than by testing the system.
"The DP auditor must get away from that type of procedure so he can become more independent of the data processing department," Haynes said. "He must be taught how to use the computers as a tool to control audits".

Audit specialist

The fourth level includes the DP audit specialist. This person needs a knowledge of systems programming. "To do an in-depth evaluation of the DP function, the auditor at this level should really know software and hardware," Haynes said.

Haynes also suggested that the auditor be involved immediately after the general design of a system to make sure that proper controls are installed. In the U.S., which has some 100,000 corporate auditors in the private sector, only about five out of 50 are DP auditors, according to IIA figures. This lack of DP experience is a major concern of the association, and this first conference is an expression of that concern.
John Fletcher, executive director of professional development for IIA, said

> "Because auditing in the past was primarily a manual procedure, the acceptance of the computer and internal control software has not come easily to "green visor" auditors".

The DP auditor "must invest in himself so as to learn the new technological techniques and be able to select the critical information needed in an organization".
"Manual auditors" may be victims of what he called the "Paul Principle," a stage in an auditor's professional development where he reaches a competent level, but fails to keep abreast of new technology. "We need one auditor - a combination of the manual and DP auditor who knows what kind of information is essential," Fletcher said.

COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.

EXTERNE CURSUSSEN; ONDERWIJS

Cursus inleiding administratieve organisatie

door drs. J.A. Beeftink

Aanleiding

In 1980 kreeg de organisatiegroep het verzoek van een cliënt om een cursus administratieve organisatie te verzorgen voor een aantal functionarissen met een administratieve functie en opleiding (MBA, HEAO en SPD).
Voor de cliënt was het van belang dat deze cursus op de bedrijfssituatie zou worden toegesneden.
Op basis van dit verzoek en met de verwachting dat gezien de toenemende informatieproblematiek in organisaties en het feit dat een aantal administratieve opleidingen slechts geringe aandacht schenken aan het onderdeel administratieve organisatie, heeft de organisatiegroep in overleg met AC en Algemene Sector besloten een cursus inleiding administratieve organisatie te ontwikkelen, welke een grotere toepassing moest krijgen dan bij één cliënt.

In-house-(bedrijfs)cursus of open cursus

Een oplossing moest worden gevonden voor de complicatie dat een specifiek voor een cliënt ontwikkelde cursus ook geschikt moest zijn voor andere cliënten. Deze omstandigheid is opgelost door vanaf de start de cursus modulair op te zetten. Al naar gelang de specifieke bedrijfssituatie kunnen modules vervallen, worden toegevoegd of zelfs speciaal worden ontwikkeld. Daar tijdens de cursus door de deelnemers een groot aantal groepsopdrachten uitgevoerd moeten worden, kan ook in de dosering van de opdrachten rekening worden gehouden met de bedrijfssituatie.

Stand van zaken

De verwachting dat ook bij andere cliënten interesse voor deze cursus zou bestaan is inderdaad uitgekomen. Sinds 1980 is de cursus nu tienmaal als in-house cursus gegeven. Voor 1981 zijn nu al zeven in-house cursussen afgesproken. De cursussen worden voor een gevarieerd aantal organisaties gegeven zoals:
- produktiebedrijven,
- rijksoverheid,
- banken,
- universiteiten, hoge scholen, academische ziekenhuizen,
- handelsbedrijven.

Naast deze in-house-mogelijkheid is in 1981 gestart met het geven een open cursus inleiding administratieve organisatie. In 1982 zal in ieder geval weer één open cursus (van 10 - 16 mei 1982) verzorgd worden, waarbij niet uitgesloten is, dat bij voldoende belangstelling in het najaar een tweede open cursus georganiseerd wordt.

Doelgroep

De cursus is niet specifiek gericht op medewerkers van interne accountantsdiensten maar richt zich op functionarissen, die direct of indirect betrokken zijn bij de informatieverstrekking of -verzorging. In het bijzonder wordt gedacht aan functionarissen die bij een onderdeel van deze cyclus een leidinggevende, initiërende, coördinerende, controlerende of adviserende rol vervullen.

De inhoud van deze cursus maakt het mogelijk dat functionarissen met voldoende praktische ervaring doch zonder theoretische vooropleiding op het terrein van de administratieve organisatie de cursus kunnen volgen.

Thema

Leidraad in deze cursus zal zijn het beheersen van de diverse structuren en processen binnen een organisatie. Uitgangspunt is dat deze beheersing veelal plaatsvindt door het instellen van een systeem van informatieverzorging en de bijbehorende rapportage.

Een dergelijk systeem zal doeltreffend moeten zijn en aan eisen van betrouwbaarheid, tijdigheid en doelmatigheid moeten voldoen. De beheersingsmaatregelen welke gewenst zijn om tot een betrouwbaar systeem van informatieverzorging te komen, zullen in deze cursus uitgebreid aan de orde komen. Daarnaast zal aandacht aan de concrete uitvoering worden besteed.

Wijze van kennisoverdracht

De cursus wordt niet gegeven als een eenzijdige kennisoverdracht van twee docenten naar de cursisten, maar de communicatie tussen cursisten onderling en tussen cursisten en docenten staat centraal.

Daartoe worden een dertigtal praktisch gerichte vraagstukken in werkgroepen uitgewerkt. Deze vraagstukken zijn over het algemeen zeer bondig en gebaseerd op reële situaties.
De ervaring leert dat ondanks de beknoptheid van de vraagstukken de groepsuitwerkingen toch dermate uit elkaar kunnen liggen dat dit tot een verlevendiging en tot inzicht in de problematiek leidt.

Programma

De cursus is opgebouwd uit vijf basismodules, waarbij bij een in-house-training veelal een zesde op de organisatie gerichte module (van meestal één dag) wordt toegevoegd. Op de inleiding na zijn de basismodules weer onderverdeeld in een aantal onderdelen die afhankelijk van de situatie kunnen vervallen of kunnen worden uitgebreid.

Bij de AC-Administratieve zaken (mevr. P.A.H. Ibrahim of de hr. H.J.M. van der Wielen) en bij het OG-Secretariaat (mevr. J.M. van Kleef), zijn brochures te verkrijgen waarin het programma van de open cursus uitgebreid staat vermeld. In dit kader zal volstaan worden met een korte schets van de achtergrond van de modules.

Basismodule 1: Inleiding

Deze module wordt iedere cursus onverkort gegeven en is gericht op het bijbrengen van een aantal basisbegrippen. Aangegeven wordt welke vraagstukken aan de orde komen bij het opzetten van de administratieve organisatie bij een onderneming. Aandacht wordt geschonken aan verschilpunten tussen de afdelingsgerichte en systeemgerichte benadering van administratieve organisatie en daarmee samenhangende informatieverzorging en procedures.

Basismodule 2: Interne controle

Deze module is het platform van de cursus. Het beheersen van een organisatie door of namens de leiding hiervan staat centraal in deze module. De problematiek van het beheersen van processen binnen een organisatie en de afstemming van deze processen op elkaar komt aan de orde. Aangegeven wordt dat deze beheersing kan plaatsvinden door een systeem van rapportage en verantwoording.
Om een betrouwbaar informatiesysteem te krijgen is een aantal interne controlemaatregelen gewenst. Deze maatregelen komen door middel van een groepswerkstuk stelselmatig aan de orde.

Binnen deze basismodule is een aantal onderdelen te onderkennen die afhankelijk van de cursussituaties kunnen vervallen en kunnen worden uitgebreid, namelijk de onderdelen:
- beschrijving en beoordeling van administratieve procedures
- interne controle bij geautomatiseerde gegevensverwerking.

Basismodule 3: De administratieve organisatie van een aantal functies en afdelingen

In deze module komen de informatieproblematiek en de maatregelen van interne controle bij een aantal te onderscheiden functies in een organisatie aan de orde, namelijk bij inkopen, verkopen, voorraden, lonen en liquiditeiten.

Basismodule 4: Typologieën van toepassingen

In deze module komt aan de orde dat binnen organisaties toepassingen zijn te onderkennen welke overeenkomsten hebben met toepassingen bij andere organisaties.

Deze toepassingen kunnen gerelateerd worden aan de goederenbeweging van een organisatie. Op deze manier kunnen toepassingen geclassificeerd worden. Meerdere van deze toepassingen (systemen) zijn veelal binnen één organisatie te onderkennen.

Een nadere nuancering van de administratieve organisatie is aan te brengen door rekening te houden met de marktgerichtheid van een organisatie. Ingegaan wordt op de kenmerken bij non-profit-organisaties, profit-organisaties en overheidshuishoudingen.
Met name bij bedrijfscursussen worden deze typologieën van toepassingen niet uitputtend behandeld, doch accenten gelegd bij de toepassing welke voor de cliënt van belang is.

Basismodule 5: Capita selecta

Bij de open cursus wordt de laatste dag besteed aan een aantal onderwerpen, welke door de cursisten naar voren worden gebracht. Hierbij bestaat de mogelijkheid dat in een parallelsessie wordt ingegaan op de problemen die in een bepaalde typologie te onderkennen zijn.
Zo'n parallelsessie kan bijvoorbeeld worden gehouden indien een groot aantal deelnemers uit eenzelfde type organisatie afkomstig zijn(bijvoorbeeld banken of non-profit-organisaties).

Basismodule 6: In-house-cursus

Deze module wordt veelal speciaal voor de cliënt ontwikkeld.

COMPACT is een uitgave van de AC-groep van Klynveld Kraayenhof & Co.