KMG Klynveld Kraayenhof & Co.
Automatisering & Controle-groep

COMPACT

Capita selecta uit
Compact nrs. 31 t/m 34
10e jaargang

ten behoeve van de Colleges Automatisering & Controle
van de Erasmus Universiteit

- Gebruik en Controle van on-line applicaties
  door J.L.H. Kooijman

- Beheersing, beveiliging en controle van het
  IBM systeem/38
  door A.H.C. Koedijk

- Continuïteit van de gegevensverwerking, een
  inleiding
  door H. Roos

- Back-up, Restart en Recovery
  (deel 1 Back-up)
  (deel 2 Recovery en restart)
  door R. Bron

- Password-protectie
  door A. van der Drift
  met tevens antwoord op de vraag van lezer

COMPACT

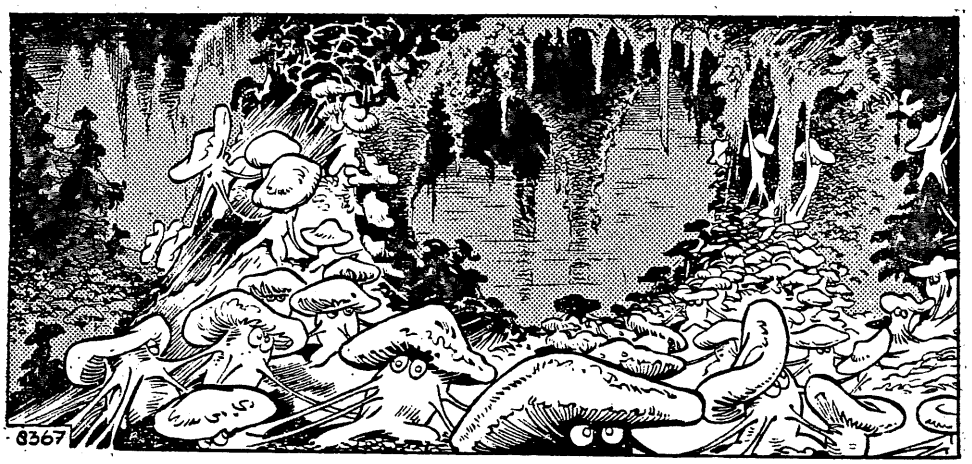
Capita Selecta uit Compact nrs. 31 t/m 34 10e jaargang

ten behoeve van de Colleges Automatisering & Controle van de Erasmus Universiteit

18 april 1986

GEBRUIK EN CONTROLE VAN ON-LINE APPLICATIES

door J.L.H. Kooijman



8367 Onder de Zwarte Bergen bevindt zich de onderwereld. Daar wonen de Kwillen, een levensvorm die nog niet door geleerden ontdekt is en daarom wetenschappelijk niet bestaat.
Het is een rustig volkje, dat een zwijgend leven leidt in de eeuwige stilte van hun holen en gangen. Want een taal bezitten ze niet en die hebben ze ook niet nodig. Onderling zijn ze namelijk verbonden door draden waardoor ze communicatie hebben; op die manier weet de een wat de ander weet, en daardoor is er nooit ruzie.

Het perfecte datadistributiesysteem.

I - Inleiding

In dit artikel wordt een overzicht gegeven van facetten die bij beoordeling en controle van on-line applicaties een rol spelen. Het gaat daarbij met name om de invloed die een on-line applicatie kan hebben op de werkzaamheden van de accountant in het kader van de jaarrekeningcontrole.
De maatregelen van interne controle die bij on-line applicaties zoal van toepassing kunnen zijn worden besproken, waarna wordt aangegeven welke mogelijkheden de accountant ter beschikking staan om een oordeel te krijgen over bestaan en werking van die maatregelen.
Allereerst een aantal opmerkingen vooraf.

- Een belangrijke richtinggevende factor bij het onderzoek van on-line applicaties wordt gevormd door de betrokkenheid van de afdeling of afdelingen (of de organisatorische functie respectievelijk functies) die de gegevens uit de applicatie gebruikt voor het voeren van de administratie.
  De complexe technologie die voor de ontwikkeling en instandhouding van de on-line applicatie wordt ingezet kan vele gebruikers voor geweldige problemen plaatsen. Die technologie is daarmee van grote invloed op de mogelijkheden die de gebruiker ziet om mee te doen bij de ontwikkeling en het testen van de applicatie, alsmede op de wijze waarop de administratieve organisatie rondom deze applicatie zou moeten worden opgezet. Uit de opzet van die administratieve organisatie zal de accountant moeten afleiden welke greep de gebruiker heeft of denkt te hebben op zijn eigen informatieverwerkend systeem. De gebruikersbenadering is daarmee van groot belang voor de aanpak van de accountantscontrole.

- Een on-line applicatie staat niet op zichzelf.
  In het kielzog van de on-line applicatie vinden wij naast de techniek van de database-, teleprocessing- en operating systemen ook nog de automatiseringsomgeving voor het management van die (algemene) software en de omringende administratieve organisatie van de gebruiker te wiens behoeve de on-line applicatie is opgezet. Zonder deze omgeving kan de on-line applicatie niet functioneren. Of het nodig is deze omgeving dan ook maar te betrekken bij het onderzoek van de on-line applicatie staat daarmee echter geenszins vast.
  Wij zullen aan deze afweging, die vooral van invloed is op de omvang van het accountantsonderzoek, ruime aandacht besteden.

- Een ander facet, dat direct samenhangt met het voorgaande is de wijze waarop de aangeleverde gegevens door de on-line applicatie worden verwerkt (verwerkingskarakteristiek).
  De techniek biedt hier onbeperkte mogelijkheden. Er zijn on-line applicaties die bij nadere beschouwing alleen data-entry omvatten, terwijl ook systemen worden aangetroffen waarbij vanaf beeldschermen rechtstreekse mutatie plaatsvindt van actuele bestanden.

Deze twee uitersten en alle tussenliggende variaties brengen hun eigen specifieke risico's mee met betrekking tot betrouwbaarheid en beveiliging.
De verwerkingskarakteristiek bepaalt daardoor in hoge mate de diepgang van het onderzoek van een on-line applicatie.
In dit artikel zullen wij hoofdzakelijk de aandacht richten op de applicaties waarbij rechtstreekse mutatie van actuele bestanden plaatsvindt.

- In het voorgaande is de term on-line applicatie al veelvuldig gebruikt en wij zijn er daarbij vanuit gegaan dat aan de lezer voldoende duidelijk is wat wij daarmee bedoelen.
  Voor de goede orde volgt hier een nadere definitie van "onze" on-line applicatie die wij in dit artikel ten tonele voeren.
  Onze on-line applicatie betreft een informatieverwerkend systeem waarbij - via geautomatiseerde hulpsystemen - beeldschermen beschikbaar zijn gesteld aan eindgebruikers. Deze zijn daardoor in staat de geregistreerde gegevens rechtstreeks te benaderen en naar eigen goeddunken direct te muteren (on-line, real-time zo u wilt). Voorts is onze on-line applicatie in de onderneming van groot belang; de bedrijfsvoering is afgestemd op de snelle en betrouwbare gegevensverstrekking uit het systeem en bij de opstelling van de jaarrekening zijn de gegevens uit onze applicatie van grote invloed.

  Dit noodzaakt een nader onderzoek naar de betrouwbaarheid van de gegevensverwerking door deze applicatie, of - beter gesteld - naar het gehele complex van administratie en organisatie, inclusief interne controle, ten behoeve van een juiste, volledige, tijdige en geautoriseerde gegevensverwerking door onze applicatie.

Wat moet er nu worden onderzocht van dit complex, met welke diepgang, in welke volgorde en op welke wijze.

In het voorgaande hebben wij kort aangegeven welke factoren een rol zullen spelen (gebruiker, automatiseringsomgeving en technologie).
De kernproblemen die voorafgaande aan de start van het accountantsonderzoek (of de EDP-audit) dienen te worden aangepakt, zijn de volgende:

1. Aanpak van het onderzoek

In hoeverre kan en mag de accountant meegaan met de aanpak die de gebruiker zelf hanteert (systeemgericht of gegevensgericht), welke overwegingen spelen daarbij een rol en welke eigen actie van de accountant kan nodig en zinvol zijn.

2. Omvang van het onderzoek

Moet de automatiseringsomgeving (het décor waartegen de applicatie wordt uitgevoerd) ook worden onderzocht? En zo ja, met welke diepgang zal dat moeten gebeuren, wat moet worden meegenomen en wat niet.

3. Diepgang van het onderzoek

Welke invloed heeft de verwerkingskarakteristiek. Kan men wellicht met een onderzoek en toetsing van enige belangrijke steunpunten volstaan, of eist de technologie diepgaand en gespecialiseerd onderzoek op vele onderdelen.

Dit artikel beoogt ideeën te geven voor de benadering van deze kernproblemen en poogt richtinggevend te zijn voor de aanpak van de controle. Voorafgaand hieraan zullen wij nader ingaan op enkele specifieke punten ten aanzien van de on-line technologie zelf en de consequenties van deze technologie voor de structuur van de interne controle.

II - On-line applicaties

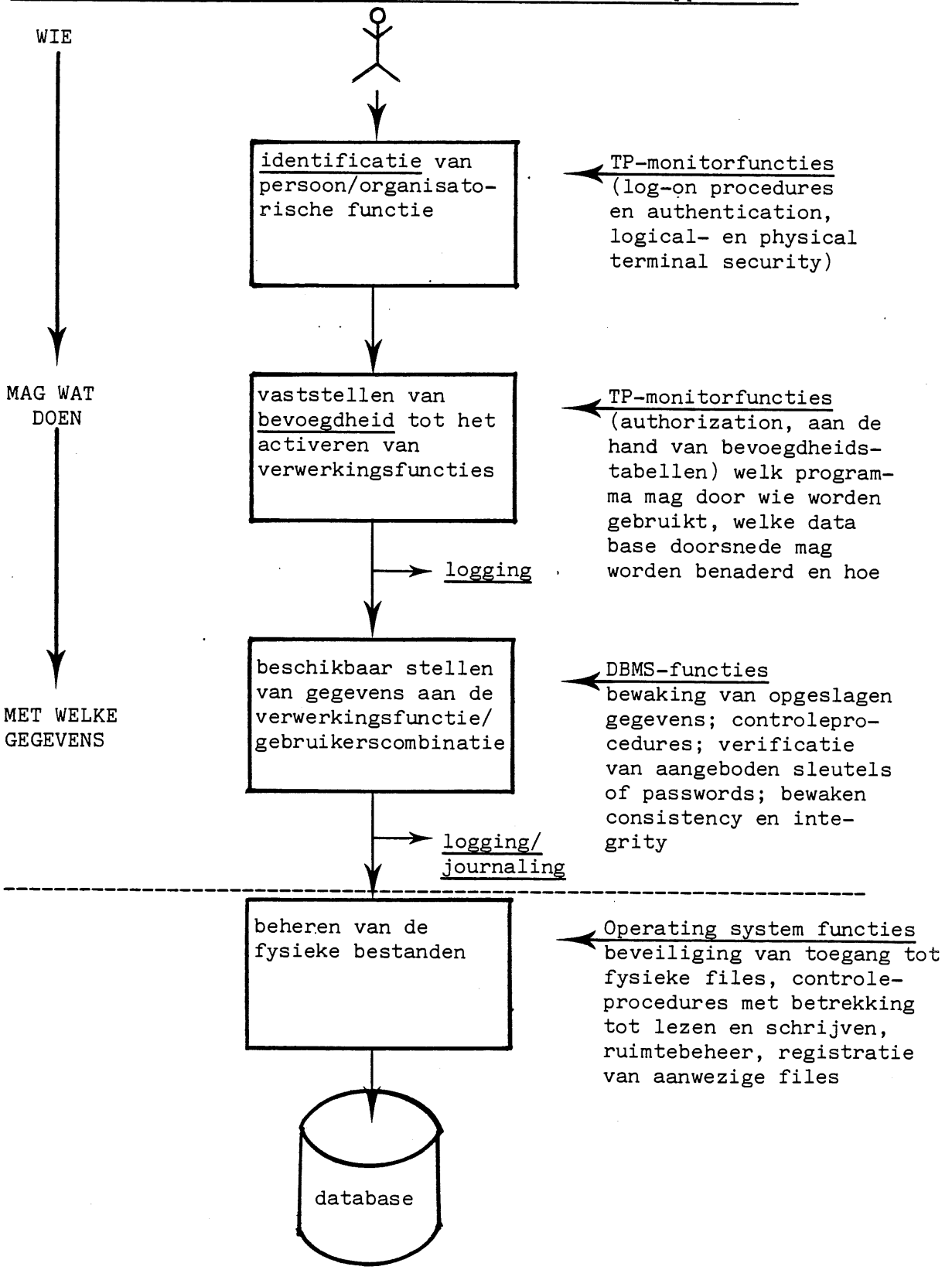
A. Technologie; algemeen

De voortschrijdende technologie heeft het mogelijk gemaakt, de automatisering veel dichter bij de gebruiker te brengen, met name door het installeren van invoer- en uitvoerfaciliteiten in de gebruikersafdelingen.
In vergelijking tot de traditionele batchomgeving heeft dit aanzienlijke verschuivingen veroorzaakt in het stelsel van interne controlemaatregelen.

De accountant staat hier voor het probleem dat bestaande controlemiddelen soms niet meer toepasbaar zijn of anders moeten worden gericht. Sommige steunpunten van interne controle zijn vervallen, ondergebracht in nieuwe organisatorische functies of vervangen door computerprogramma's.
Wij zullen nagaan welke de belangrijkste invloeden zijn van de on-line applicatie op het stelsel van interne controle.
Onze belangstelling richt zich daarbij op onze applicatie waarbij met behulp van database-management systemen en teleprocessing-monitoren, de gegevensinvoer en bestandsbewaking plaatsvindt en van directe bestandsmutatie sprake is.

De belangrijkste componenten van deze systematiek zijn in het hierna volgende schema met toelichting weergegeven.

Componenten en faciliteiten ten behoeve van on-line applicaties



Toelichting

Wie mag wat doen met welke gegevens

Interne controle ') wordt voornamelijk gerealiseerd door toepassing van functiescheiding, gevolgd door afstemming van de resultaten. Bij de controle van administratieve processen wordt dan ook altijd voor de belangrijkste activiteiten de functiescheiding nagegaan en beoordeeld. Het onderzoek naar de opzet en de betekenis van functiescheidingen is in de traditionele administratie niet al te ingewikkeld; door raadpleging van organisatieschema's en functiebeschrijvingen (taken, bevoegdheden) kan hierin een goed inzicht worden verkregen. Bestaan, handhaving en naleving van de functiescheidingen kunnen worden vastgesteld met behulp van een scala van controletechnieken.
Wanneer echter voor de gegevensverwerking gebruik wordt gemaakt van on-line systemen, wordt met name de toetsing van handhaving en naleving moeilijker. De accountant zal, met andere woorden, moeten vaststellen of het stelsel van functiescheidingen ook bestaat in het geautomatiseerde systeem en of het toezicht op de handhaving van dit stelsel naar behoren functioneert en gefunctioneerd heeft.
In de hiernaast opgenomen schets is aangegeven welke faciliteiten er ten behoeve van on-line applicaties aanwezig zijn om toezicht te kunnen uitoefenen op het gebruik van verwerkingsfuncties en het benaderen van gegevens. Deze faciliteiten zijn algemeen van aard en in standaardsoftware aanwezig (general controls). De verantwoordingsregistratie (logging, journaling, audit-trail) wordt door deze standaardsoftware geleverd. Deze verantwoordingsregistratie kan - aangezien per applicatie de gegevens ten behoeve van de functiescheiding aan de standaardsoftware worden gegeven - mede bruikbaar zijn voor de toetsing van de handhaving en naleving van deze functiescheidingen. De per applicatie aanwezige identificatie en autorisatietabellen zijn derhalve bruikbaar voor de vaststelling van het bestaan van de gewenste functiescheidingen voor de applicatie.

In de schets is tevens aangegeven, welke controlestations achtereenvolgens moeten worden "genomen" voordat een gebruiker gegevens kan benaderen. Wij hebben daarbij de vraag gesteld: wie mag wat doen met welke gegevens.

') Met "interne controle" bedoelen wij de in de administratieve en organisatorische procedures ingebouwde waarborgen met betrekking tot autorisatie, volledigheid, juistheid en tijdigheid van informatie en met betrekking tot de beveiliging van bezittingen, alsmede het geheel van maatregelen dat getroffen wordt bij afwijkingen ten opzichte van gestelde regels of normen.

De accountant zal in het kader van zijn controle-arbeid ten aanzien van deze vraag de volgende nuancering aanbrengen:

1. Wie zou wat mogen doen met welke gegevens.
   Dit geeft de eigen beoordeling weer van de accountant, gegeven de omvang van de interne organisatie, het type toepassing en de daarbij aanwezige functies.

2. Wie mag wat doen met welke gegevens.
   Dit betreft de vaststelling dat de beoogde functiescheidingen ook in het geautomatiseerde systeem aanwezig zijn.

3. Wie heeft wat gedaan met welke gegevens.
   Hier is de vaststelling van de goede werking van het systeem aan de orde. Als het goed is, wordt dit door de gebruiker aan de hand van de applicatie-uitvoer gecontroleerd; aanvullende faciliteiten uit de standaardsoftware zijn logging, journaling en audit trails.

Alvorens nader in te gaan op de mogelijkheden voor het beoordelen en toetsen van de in de applicatie aanwezige functiescheidingen, zullen wij nagaan welke verschuivingen in het stelsel van interne controlemaatregelen worden veroorzaakt door de on-line technologie.

B. Invloed op de structuur van de interne controle;
gevolgen voor de accountantscontrole

Als gevolg van de toegepaste technologie (databases, TP-monitoren) treden verschuivingen op in de vormgeving van de maatregelen van interne controle.
Deze verschuivingen en de invloed daarvan zijn als volgt samen te vatten:

1. De beheersing van de gegevensverwerking en de controle daarop wordt in toenemende mate overgenomen door standaardsoftware zoals DBMS en operating systems. Dit betekent een verschuiving van application controls naar general controls.
   De controle op de betrouwbaarheid en toepassing van deze standaardsystemen zal dienovereenkomstig moeten verschuiven.
   In zeer vele gevallen zal een application-audit niet meer kunnen worden uitgevoerd zonder dat ook ruime aandacht wordt besteed aan de standaardsoftware met behulp waarvan de on-line applicatie wordt uitgevoerd.

2. Autorisatiecontroles, waarin voorheen door organisatorische maatregelen en procedures werd voorzien, zijn nu grotendeels geautomatiseerd en ondergebracht in TP-monitor, DBMS, operating system, file control systems en library pakketten.

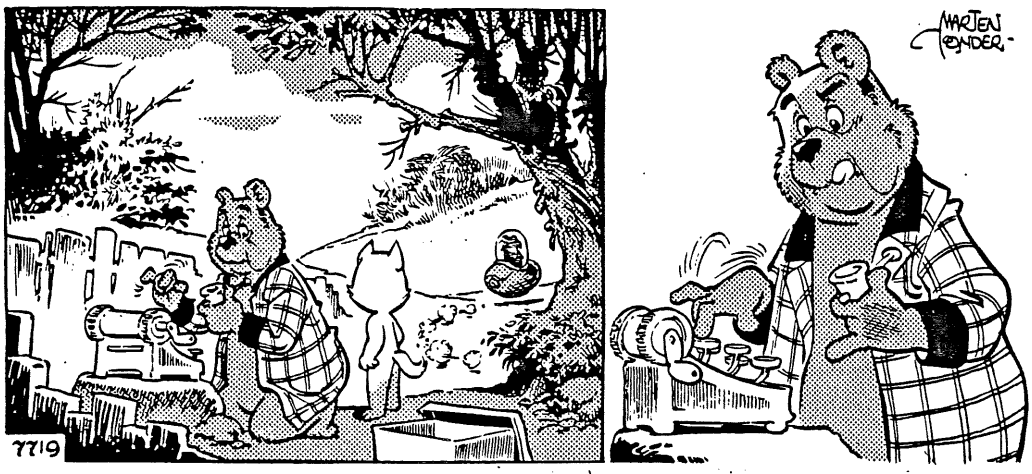
   Als voorbeeld moge dienen, het invoertraject dat bij de traditionele batchsystemen werd afgelegd langs verschillende rekencentrumafdelingen en met behulp van diverse opdrachtformulieren. Een dergelijk traject leent zich bij uitstek voor lijncontroles en proceduretests.

   De zojuist genoemde software wordt veelal slechts door één óf enkele personen beheerd en de registratie van de werking is meestal technisch gericht.
   Bij de uitvoering van het accountantsonderzoek levert dit punt vaak de grootste problemen op. De vastleggingen (logging, journaling en audit trails) zijn meestal niet erg "accountantsvriendelijk" en de vaststelling van de volledigheid van deze vastleggingen is geen geringe opgave.

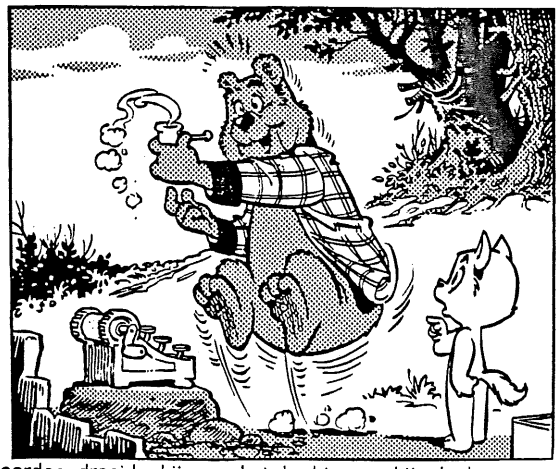
3. Een belangrijke steun voor de accountant in de traditionele batchomgeving was de aanwezigheid van aparte bestanden per applicatie en het feit dat de batchprogramma's waren gericht op de uitvoering van een afgeronde verwerkingsfunctie (een bepaald administratief proces).
   Het gebruik van het bestand en de bijbehorende programma's kon derhalve door, en voor de verantwoordelijke gebruiker/eigenaar worden gevolgd, getest, geadministreerd, etc.
   In on-line applicaties waarbij een database wordt gebruikt, is het mogelijk om gegevens aan meerdere gebruikers ter beschikking te stellen (data-sharing). De programma's zijn nu gericht op het uitvoeren van enkelvoudige opdrachten (stapjes in het administratief proces) teneinde aanvaardbare responsetijden te verkrijgen. Meestal worden ook de programma's voor gemeenschappelijk gebruik opgezet (program-sharing).
   De data-sharing en program-sharing kan het stelsel van functiescheidingen ernstig bedreigen, als hiervoor in de systemen geen toereikende bewakingsmechanismen zijn opgezet.
   Daarbij is de gegevensverwerking een continu proces geworden. Waren er bij de batchsystemen heldere meetpunten (de "batch", zie ook 2); in het on-line systeem worden verwerkingsopdrachten onmiddellijk gehonoreerd.
   In deze nieuwe omgeving zullen dan ook nieuwe technieken moeten worden toegepast om het bestaan en de werking van de functiescheidingen na te kunnen gaan.

III - De voorbereiding op het onderzoek

Een van de kernpunten voor de uitvoering van het onderzoek betreft de vraag naar de aanpak.
In het voorgaande hebben wij dat verbonden met de manier waarop de gebruiker omgaat met het geautomatiseerde systeem en op welke wijze hij vaststelt dat het doet wat het moet doen. Ter illustratie hiervan zien wij hieronder zo'n gebruiker.



„Een transmieter," sprak hij tot zichzelf. „Nooit van gehoord. Het lijkt me het beste, dat ik eens ga proberen hoe zo'n ding werkt. Wat heb ik in de gauwigheid nodig?"
Dat was een moeilijke vraag voor een heer, die eigenlijk alles al heeft. Maar toen zijn blik op zijn lege pijp viel klaarde zijn peinzend gelaat op, en hij begon te tikken.
„Waar komt die schrijfmachine vandaan?" vroeg Tom Poes.
„Stoor me niet," mompelde heer Ollie, voorzichtig op de toetsen drukkend. „Ik bestudeer deze bestelling. En dat is héél moeilijk omdat er zo weinig letters op staan. Even kijken. Juist, ja, zo kan het... Tabak in mijn pijp wordt: tapac in myn pyp. Heel duidelijk."



Met deze woorden draaide hij aan het krukje, en hij slaakte een verheugde uitroep toen er plotseling een rookspiraaltje uit zijn pijpekop steeg.
„Het is gelukt," zei Tom Poes verbaasd. „Een vreemd toestel, hoor. U had hem toch niet besteld? Dat zei u zelf daarnet.
„Zeur niet!" riep Heer Bommel opgetogen. „Hij is van mij, al was de adressering een beetje fout met die nul achter mijn naam. Maar hij is aan het juiste adres afgeleverd; dat zal je met me eens zijn, jonge vriend!"

Gebruikers van on-line systemen; omgaan met geavanceerde techniek of: Hoe Een Gebruiker Iets Groots Accepteert Op Grond Van Een Kleinigheid.

A. Gebruikers

Afgezien van de acceptatieprocedure, waarvan het van belang is na te gaan op welke wijze de gebruiker de verantwoordelijkheid voor het informatiesysteem heeft overgenomen van de ontwerpers, zal de accountant moeten onderzoeken hoe de gebruiker vaststelt dat de gegevens die uit het systeem komen, correct zijn en welke maatregelen de gebruiker in gang zet als de computer - door welke oorzaak dan ook - zou uitvallen. Dit initiële onderzoek is van groot belang voor het verdere verloop van de accountantscontrole. Wij zullen daarom even stilstaan bij de problemen die de gebruiker ontmoet wanneer hij zijn (geautomatiseerde) administratie onder controle wenst te houden.

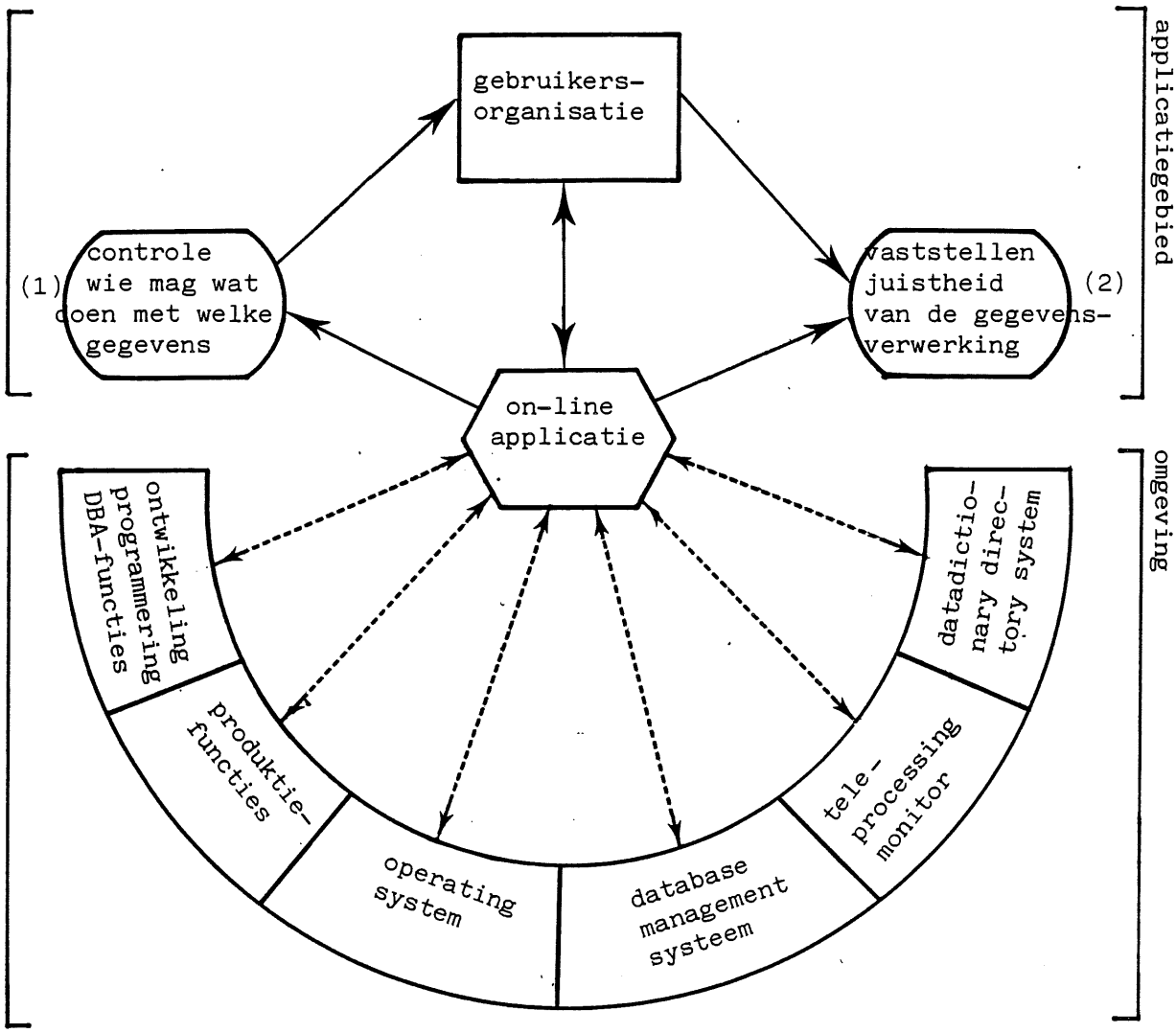
- De vertrouwde "masterbestanden" zijn ondergebracht in een grote database waarvan hij niet meer het exclusieve gebruiksrecht heeft.

- Het stapeltje ponsconcepten, de ponskaarten en het mutatiebestand (de "batch") is verdwenen en de route van deze batch door afdelingen en systemen valt als steunpunt weg.
  Het volgen van een enkele transactie door het systeem, vanaf beeldscherm tot in database en op overzichten is voor een gebruiker veel moeilijker.

- Het batchprogramma dat als afgerond geheel van verwerkingstaken gericht kon worden getest, uitgeprint of in blokschema's zichtbaar kon worden gemaakt, is nu vervangen door vele kleine TP-programma's die tijdens een beeldschermconversatie door de TP-monitor worden opgeroepen en verbonden om na de uitvoering van de transactie weer te verdwijnen in een "programmapool".

- De rubriekscontroles, validaties en opmaakroutines die vroeger door het batchprogramma werden uitgevoerd zijn nu ondergebracht in de standaardsoftware van het DBMS.
  Welke controles nu precies voor een bepaalde gebruiker aanwezig zijn, valt moeilijker na te gaan en vereist een goede rapportage van hen die het DBMS beheren.

Een minder geïnteresseerde gebruiker is dan ook geen ongewoon verschijnsel. Wij moeten daarbij tevens bedenken dat de betrouwbaarheid van de gegevensverwerking door een on-line applicatie niet meer van één enkele gebruiker afhankelijk is. Wanneer in een kring van gebruikersafdelingen er één is, waar met controle en beveiliging minder gewetensvol wordt omgegaan, zal dit van grote invloed zijn op de betrouwbaarheid van de informatie die in het totale systeem is opgeslagen en het kan tevens leiden tot een ernstige verzwakking van het toegangsbeveiligingssysteem.



B. Onderzoekgebied.

Een en ander impliceert dat de greep die een afzonderlijke gebruikersafdeling heeft op de betrouwbaarheid van zijn eigen applicatie, in principe geringer is dan die in de traditionele batchomgeving.
Dit houdt ook in - en dat is van groot belang voor de aanpak van de EDP-audit - dat de controle van de afzonderlijke applicatie (de application-audit) van minder betekenis is geworden voor de beoordeling van betrouwbaarheid en continuïteit van de gegevensverwerking ten behoeve van de betrokken gebruiker.
De applicatie als zodanig speelt voor deze facetten daarbij een te geringe rol.

B. Onderzoekgebied

Wij menen dat met betrekking tot de afzonderlijke applicatie er voor het accountantsonderzoek nog maar twee facetten van belang kunnen zijn, te weten:

1. De voor die bepaalde applicatie aanwezige verwerkingsbevoegdheden.

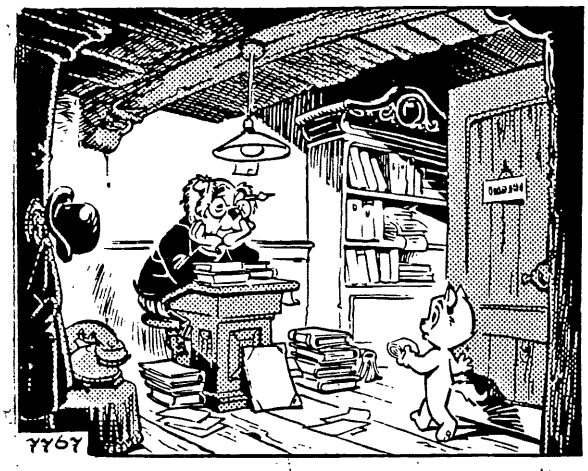
2. Controle op de verwerking zelf wanneer geen goede relatie aanwezig is tussen invoer en uitvoer.

Ten behoeve van de beeldvorming vatten wij het onderzoeksgebied hiernaast samen in twee blokken: het applicatiegebied en de omgeving die zorgt dat de applicatie kan functioneren.

C. Aanpak van het onderzoek, audit-strategy

We kennen de gegevensgerichte en systeemgerichte controle-aanpak.
Veel schrijvers adviseren een systeemgerichte aanpak wanneer sprake is van geavanceerde automatisering en een gegevensgerichte aanpak bij kleine geïsoleerde (mini/microcomputers) omgeving. Veelal wordt daarbij het keuzeprobleem voor de ene of andere richting versoepeld door het advies, met een mengvorm van beide benaderingen te werken.
In dit artikel zal dit laatste, de mengvorm, eveneens aan de orde komen.
Daarom staat centraal de benadering van de gebruiker van het systeem, waarbij moet worden nagegaan of die benadering adequaat is gegeven de systeemtypologie.
Wanneer die benadering toereikend is zal de accountant die in het algemeen moeten volgen, tenzij dit zou leiden tot grote ondoelmatigheden óf onnodig hoge controlekosten.

In grote lijnen zal de vaststelling van de wijze van aanpak, uitvoering en diepgang als volgt verlopen.



7767. De heer Dorknoper bevond zich in grote moeilijkheden. Het uitzoeken van de fouten, die door de stadsrekenmachine gemaakt waren, zou tweeduizend beambten gedurende twintig jaren van werk kunnen voorzien. En hoewel de ambtenaar eerste klasse heel wat aankon, begreep hij toch, dat hij hier voor een onmogelijke taak stond.

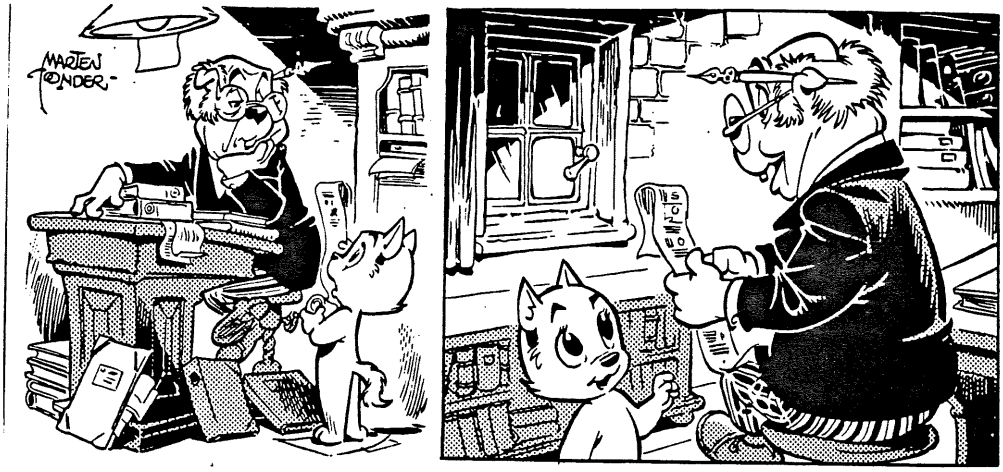
„Als ik nu maar wist, waar de fout begonnen is," zei hij somber tot zichzelf. „Toen we de heer Bommel verdachten, konden we in de OBB-lijn zoeken. Maar die vertoont geen afwijkingen, zegt referendaris Kreut."

Hij zuchtte diep en wendde zich tot Tom Poes, die met een rolletje papier binnen was gekomen.

„Ik heb geen tijd," sprak hij knorrig. „U gelieve zich aan de officieel vastgestelde spreekuren te houden. Goede dag."

„Hier staat alles op," zei Tom Poes. „Alles wat de transmieter gedaan heeft. Maar het is gedrukt in een soort onleesbare code."

Zo sprekende overhandigde hij de dropslip aan de heer Dorknoper, en deze wierp



er een onthutste blik op.

„Onleesbare code?" herhaalde hij. „Dat is voor ons geen bezwaar. We kunnen gewoon de computer inschakelen, die de ambtelijke taal ontwerpt. Maar hoe komt u aan deze lijst, meneer Poes? Is het mogelijk dat de heer Bommel er toch iets mee te maken heeft?"

„Iets," gaf Tom Poes toe. „Maar buiten zijn schuld, dat zult u wel merken wanneer u dit ontcijfert, denk ik. Het was allemaal een vergissing."

De hooggeplaatste klerk begreep weinig van deze uitleg, maar hoe langer hij naar de papierstrook keek, hoe meer hij opklaarde.

„Dit is het!" verklaarde hij stralend. „Nu komen we er wel uit."

Logging

Vaak gebruikersonvriendelijk maar van grote waarde voor achteraf-controles, uitzoeken en herstellen van fouten.

1. Onderzoek gericht op de desbetreffende on-line applicatie

- Op welke wijze en met welke middelen stelt de gebruiker de juistheid en volledigheid van de gegevensverwerking vast (algemeen accountant).
- In welk totaalverband functioneert de betreffende applicatie; is er sprake van program- en data-sharing; zijn er verbanden met andere applicaties (EDP-auditor).

2. Vaststellen gebruikersaanpak (algemeen accountant en EDP-auditor)

- De gebruiker steunt volledig op eigen stelsels van interne controle; invoertellingen (hash- en batchtotals) worden vooraf gemaakt, aansluiting van alle uitvoer en interfaces met de eigen "schaduw"administratie vindt plaats ..... of:
- De gebruiker steunt volledig op de maatregelen van interne controle in het geautomatiseerde systeem en de automatiseringsomgeving. De invoerstroom wordt achteraf niet integraal afgestemd met de brondocumenten.

3. Beoordelen gebruikersaanpak (algemeen accountant en EDP-auditor)

In deze stap wordt nagegaan, of de accountant in principe mee kan gaan met de gebruikersbenadering.
Het controlebelang staat hier voorop. Een enkel voorbeeld ter verduidelijking van de voorwaarden die daarbij gelden:

. De accountant moet achteraf kunnen nagaan of de controles ook in werkelijkheid hebben plaatsgevonden; het ontbreken van audit-trails, journaling- of logging-gegevens blokkeert de mogelijkheden om achteraf na te gaan of een belangrijke, zogenaamde "onvervangbare" controle naar behoren heeft gewerkt.
. In een omgeving waarbij gemeenschappelijk gegevensgebruik (data-sharing) aan de orde is, zullen alle gebruikers in beginsel eenzelfde controlebenadering moeten hanteren om te voorkomen dat de situatie ontstaat van de ketting met de zwakke schakel erin.

Deze stap is een belangrijke en kan zelfs leiden tot onmiddellijke advisering

- aan alle gebruikers (via een gebruikersbeheersgroep of een data-administrator) en
- aan de automatiseringsafdelingen, alsmede

voor beide groepen betrekking hebbend op richtlijnen voor de inrichting van de administratieve organisatie respectievelijk de voorwaarden waaraan ingebouwde controles en uitvoeroverzichten zouden moeten voldoen.

D. Een gegevensgerichte gebruikersbenadering

Behalve het verband met de overige gebruikersbenaderingen in een "shared" omgeving is hier de aard van de applicatie zelf van belang. Wanneer bijvoorbeeld niet-financiële gegevens worden ingevoerd en door het systeem worden omgezet in financiële gegevens (bijvoorbeeld premieberekeningen) dan is de juiste werking van het programma waarin de rekenregels worden uitgevoerd, niet in de greep van deze gebruiker. Die zal immers met behulp van zijn registraties alleen de volledigheid van de verwerking van de kwantitatieve gegevens (aan de hand van aantallen records invoer/uitvoer) kunnen vaststellen.
Voor programma's die salarissen, rente of actuariële gegevens berekenen geldt hetzelfde.
In deze gevallen zal de gebruiker over aanvullende middelen moeten beschikken om de juistheid van deze gegevensconversie te kunnen vaststellen.
De accountant zal moeten aandringen op de ingebruikname van deze middelen of (wanneer zij in gebruik zijn) de toereikendheid en betrouwbaarheid daarvan moeten nagaan.
Het werk voor de EDP-auditor in deze omgeving kan beperkt blijven. Wanneer vastgesteld kan worden, dat deze gebruikersbenadering geen risico's oplevert voor de andere applicaties en gebruikers, zal kunnen worden volstaan met enkele deel-onderzoeken van geringe omvang. Deze betreffen de gegevensuitwisseling met andere applicaties (de interfaces) en de checks die de overige applicaties op de uit deze toepassing opgeleverde gegevens uitvoeren, alsmede de procedures van bestandsbewaking van de voor deze gebruiker aanwezige gegevensverzamelingen.

Een basis voor de uitvoering van lijncontroles en proceduretests met betrekking tot de gebruikerscontroles door de algemeen accountant ligt hiermee binnen bereik. Ook de toepassing van audit-programmatuur ten behoeve van steekproeven, bestandsonderzoek en herhaalde verwerking is mogelijk.

E. Een systeemgerichte gebruikersbenadering

Een belangrijke stap is hier het onderzoek naar de toereikendheid van de middelen die de gebruiker voor deze benadering ter beschikking heeft en de steunpunten in de interne controle die daarmee worden getoetst.
Een voorbeeld:
In het systeem bevinden zich tabellen waarin bevoegdheden van personen c.q. organisatorische functies zijn vastgelegd. De handhaving van het stelsel van functiescheidingen staat of valt met de juistheid van deze tabel, het goede gebruik ervan door het systeem en de procedures en controles met betrekking tot beheer en mutatie van de tabelgegevens.
De bewaring en registratie van de tabelgegevens is doorgaans gedelegeerd (welke gebruiker heeft dit bewust gedelegeerd?) aan de automatiseringsafdeling. De mutatiebevoegdheid blijft uiteraard bij de gebruiker.
Het is duidelijk, dat aan een gebruiker, die ten behoeve van de handhaving van de door hem gewenste functiescheidingen, gaat steunen op de administratieve organisatie en interne controle in de automatiseringsafdeling, op behoorlijke wijze hierover verantwoording moet worden afgelegd.

De EDP-auditor zal moeten beoordelen of van een goede verantwoordingsrapportage sprake is en moeten nagaan op welke wijze de rapportage tot stand komt, c.q. welke functiescheidingen daarbij bestaan.

Het onderzoek naar de toereikendheid van de middelen die de systeemgerichte gebruiker hanteert, zal veelal een omvangrijke EDP-audit met zich brengen.

Deze EDP-audit is in onze visie primair gericht op het onderzoek naar de maatregelen die aanwezig zijn ter handhaving van de functiescheidingen zoals die door de gebruikers binnen de on-line applicatie worden gewenst.
Vanuit dit centrale onderzoek (transactie-analyse), zuiver gericht op de desbetreffende on-line applicatie, wordt bepaald welke onderdelen van de automatiseringsomgeving ("general controls") voor nader onderzoek in aanmerking komen. De aanpak van het onderzoek staat nu in grote lijnen vast; omvang en diepgang zullen worden bepaald nadat de transactie-analyse is voltooid.

IV - De uitvoering van het onderzoek

A. Transactie-analyse

De transactie-analyse wordt uitgevoerd in een systeemgerichte controleaanpak. Het onderzoek is erop gericht gegevens te verzamelen aangaande functiescheidingen zoals die in de applicatie aanwezig zijn of voor de applicatie in stand moeten worden gehouden.
Het doel is verband te leggen tussen de gebruikersbevoegdheden en de bevoegdheden die in de on-line applicatie zijn vastgelegd.

De onderzoekmethode is op de volgende uitgangspunten gebaseerd:
1. Gegevens in een database kunnen uitsluitend worden benaderd door middel van speciaal daarvoor geschreven programma's (transactieprogramma's of TP-programma's).
2. De transactieprogramma's kunnen alleen met behulp van beeldschermcommando's worden gestart door daartoe bevoegde gebruikers.

(Uiteraard zijn hierop uitzonderingen; een technicus kan via speciale commands de database rechtstreeks benaderen en de operator zal - ook in on-line systemen - nu en dan wel eens een batchprogramma starten hetwelk meestal niet aan de TP-monitor controles wordt onderworpen.)

Transactieprogramma's en beeldschermfaciliteiten vormen derhalve de kern van het onderzoek. Voor elke on-line applicatie moet zijn geregistreerd welke transactieprogramma's door wie kunnen worden gebruikt. Door van deze registratie uit te gaan, kan worden vastgesteld, hoe de functiescheiding van de gebruikersorganisatie in de bijbehorende on-line applicatie is verankerd.
De procedure hiervoor is als volgt.

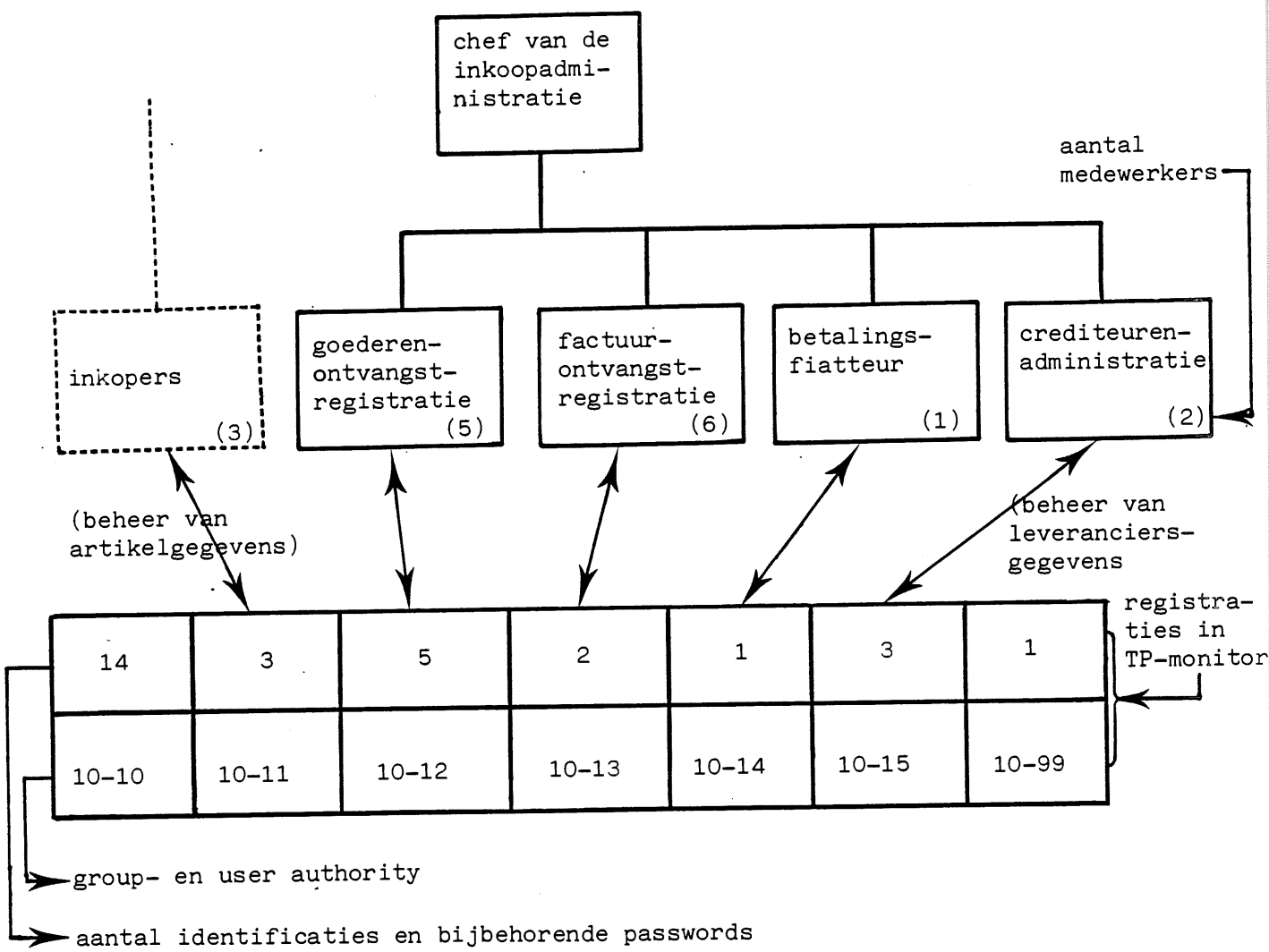
. Welke gebruikers.

1. De eerste stap is het onderzoeken van de organisatorische opbouw van de gebruikersafdeling en het vastleggen van de daarin aanwezige functiescheidingen, c.q. relevante functies.
   Parallel hiermee loopt de beoordeling van de aanwezige administratieve organisatie en de daarin aanwezige maatregelen van interne controle.
   Hierdoor kan al een indruk worden verkregen met betrekking tot de risico's van functievermenging die vanuit die organisatie zelf, al aanwezig zijn (omvang, structuur, sfeer, leiding, etc.).

2. Nu volgt de vastlegging van de aan die afdeling c.q. gebruikers verstrekte beeldschermfaciliteiten (TP-Monitor).
   Hierbij gaat het erom, vast te leggen welke gebruikers in het systeem zijn geregistreerd en over welke bevoegdheden elke gebruiker beschikt.
   Doorgaans zijn de bevoegdheden in een aantal niveaus of klassen aangegeven.

Een eerste beoordeling van de verzamelde informatie kan al in dit stadium worden uitgevoerd. Er kan bijvoorbeeld nagegaan worden of de bevoegdheidsverdeling zoals die blijkt uit zogenaamde user- classes of authority-codes aansluit met de afdelingsopbouw. In een voorbeeld hebben wij de eerste twee stappen nader uitgewerkt (figuur 1).

Figuur 1. Voorbeeld afdelingsopbouw versus systeembevoegdheden.



De aldus opgezette registratie geeft al een eerste indruk van het verband tussen bevoegdheden die met betrekking tot de desbetreffende online applicatie zijn vastgelegd in de TP-monitor en de eigenaar/gebruiker (user-groep 10).
Bevindingen:

- Zo zijn er aparte bevoegdheidsklassen in het systeem aanwezig die aansluiten op de organisatorische functies van de afdelingen (maar voor welke afdelingen of personen zijn de klassen 10-10 en 10-99 aanwezig?).
- De password-toepassing lijkt hier en daar niet helemaal in orde; bij de factuurontvangstregistratie worden twee passwords door 6 medewerkers gedeeld en bij de crediteurenadministratie is één password te veel aanwezig (van een ex-medewerker?).
- Overigens is er in de opzet van de gebruikersorganisatie zelf de primaire functiescheiding tussen de goederen en geldbeweging niet aanwezig.

. Welke verwerkingsmogelijkheden.

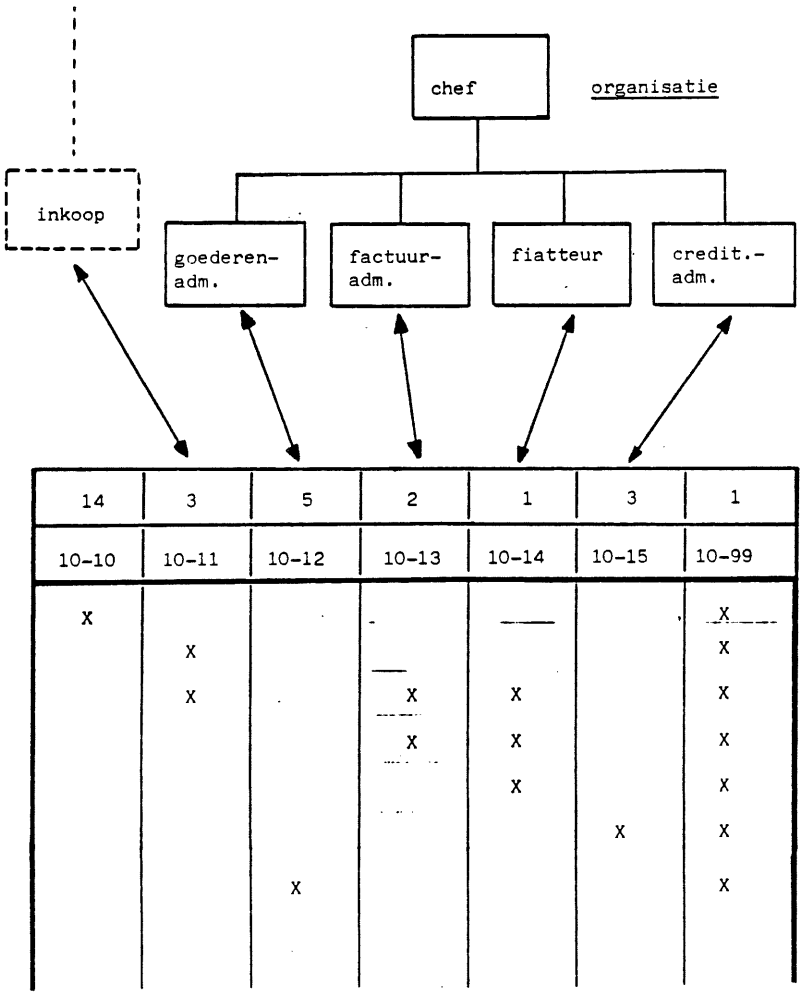
Een belangrijke volgende stap is nu de vraag wat men met deze bevoegdheden kan doen in het systeem.
Stappen 1 en 2 laten ons als het ware de inhoud van de sleutelkast zien, nu moet worden nagegaan welke deuren met de sleutels kunnen worden geopend.

Stap 3. In deze stap moet worden vastgelegd welke bevoegdheid nodig is voor het uitvoeren van een bepaald transactieprogramma.
Dit is doorgaans vastgelegd in de TP-monitor zelf of bij elk transactieprogramma afzonderlijk.
Stel dat na uitgebreid onderzoek van de bibliotheek met geautoriseerde programma's de volgende transactieprogramma's worden gevonden.

Progr. nr.	Benodigde authority	Omschrijving
01	10-10	Algemeen inquiry
02	10-11	Muteren artikelgegevens algemeen
03	10-11/13/14	Muteren artikelprijzen
04	10-13/14	Factuurgegevens wijzigen
05	10-14	Facturen fiatteren
06	10-15	Muteren leveranciersgegevens
07	10-12	Goederenontvangst vastleggen
	etc.	etc.

Door toevoeging van deze gegevens aan ons voorbeeld en het leggen van de verbindingen tussen de terminals en de programma's, ontstaat informatie waar we wat aan hebben:
"wie kan wat doen" (zie figuur 2).

Figuur 2. Transactieprogramma's.



14	3	5	2	1	3	1
10-10	10-11	10-12	10-13	10-14	10-15	10-99
X						X
	X					X
	X		X	X		X
			X	X		X
				X		X
					X	X
		X				X

Beschikbare verwerkingsfuncties

Benodigde authority	Programma-omschrijving	Progr. nr.
10-10	Algemeen inquiry	01
10-11	Muteren artikelgegevens alg.	02
10-11/13/14	Muteren artikelprijzen	03
10-13/14	Factuurgegevens wijzigen	04
10-14	Facturen fiatteren	05
10-15	Muteren leveranciersgegevens	06
10-12	Goederenontvangst vastleggen	07
	Etc.	-

In de praktijk zal deze kruisjeslijst aanzienlijk groter zijn en hopelijk ook wat minder eigenaardigheden bevatten.
Hoewel we nog niet precies weten welke gegevens in de database kunnen worden gemuteerd, kunnen toch al uit de programma-aanduidingen en de kruisjeslijst enige voorlopige conclusies worden getrokken.
Zo kan iemand die factuurgegevens behoort vast te leggen, blijkbaar ook artikelprijzen wijzigen. Met die artikelprijzen is toch het een en ander aan de hand, want niet minder dan drie afdelingsfuncties kunnen hierin muteren. Op het eerste gezicht lijkt dit niet wenselijk, etc. etc.

Elke kolom geeft voorts een volledig beeld van de taken die aan een bepaalde functie of functionaris blijkbaar zijn toegewezen; zo heeft de betalingsfiatteur veel meer mogelijkheden dan men op het eerste gezicht zou denken. Raadpleging van de functiebeschrijving lijkt hier nodig.

. Welke gegevens.

Welke gegevens kan men nu benaderen en wat kan met de gegevens worden gedaan.

In stap 4 moet worden vastgelegd wat elk transactieprogramma in de database kan uitrichten.
Dit lijkt een omvangrijk karwei, doch de ontwerpers van het DBMS hebben in de meeste gevallen verbindingsmechanismen gemaakt waarvan we in het onderzoek gebruik kunnen maken.

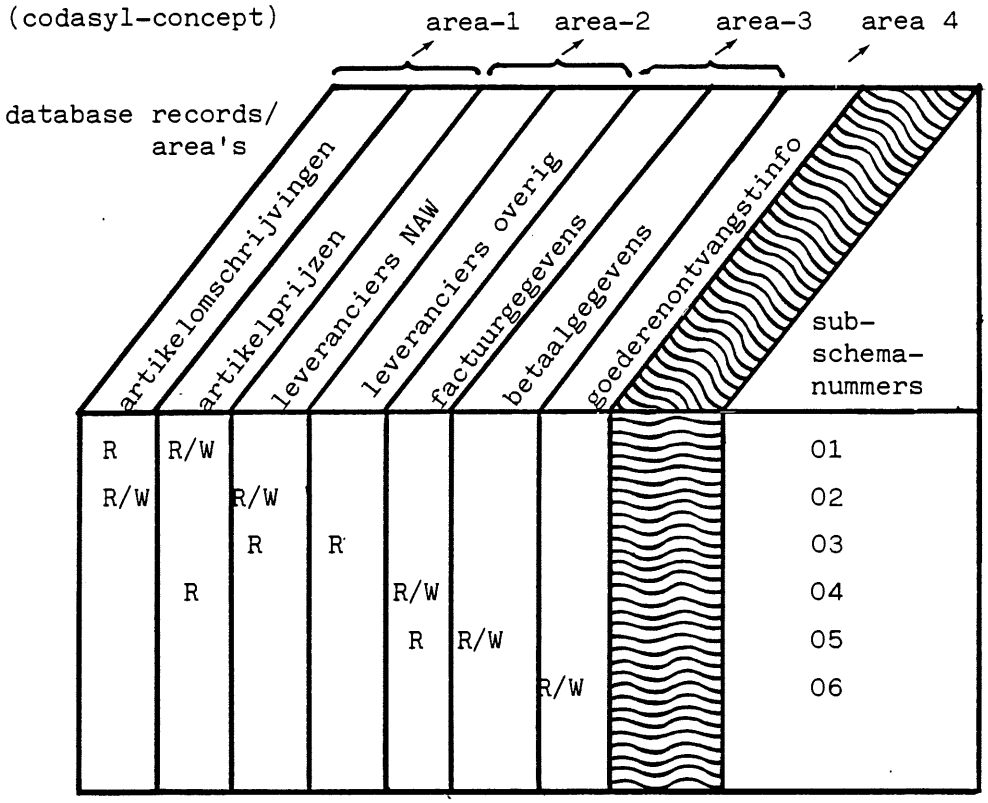
In een DBMS bestaan faciliteiten waardoor deelverzamelingen kunnen worden gemaakt uit de aanwezige gegevens. Zo'n deelverzameling wordt bijvoorbeeld subschema genoemd.
In een subschema kan nauwkeurig worden beschreven welke gegevens daarmee kunnen worden bereikt en welke manipulaties (lezen, schrijven, update, etc.) mogen worden uitgevoerd.
Een programma kan uitsluitend met de database communiceren via een subschema.
Wanneer wij dus weten welke subschema's er zijn en welke programma's van een subschema gebruik maken, weten we ook wat elk programma met de gegevens kan doen.

Net als bij de terminalfaciliteiten kan hier worden gesproken van sleutels die toegang geven tot opgeslagen database-gegevens.
Het subschemanummer is de sleutel, het verbindingselement tussen programma en database.

Een voorbeeld van een mogelijke indeling van een database is hierna opgenomen. De mate van detaillering kan van geval tot geval verschillend zijn. Dit hangt af van de vraag welke gegevens in het kader van het onderzoek van belang zijn.

Voorbeeld database onderverdeling

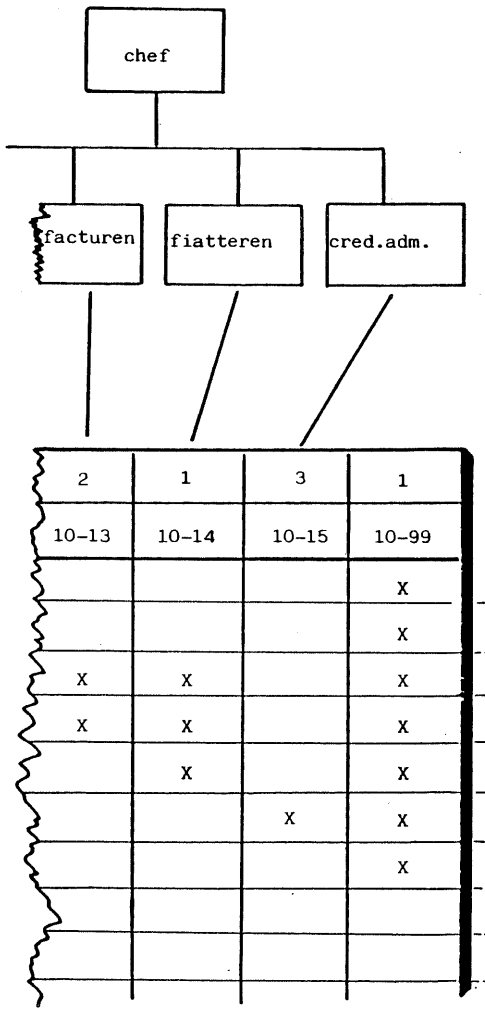
(codasyl-concept)



R = READ, W = WRITE

In dit geval is aangegeven hoe de recordonderverdeling van de database eruit ziet, welke records kunnen worden bereikt door de aanwezige subschema's en welke verwerkingsopties via die subschema's kunnen worden uitgevoerd.
Bij kritische deelverzamelingen (bijvoorbeeld financiële gegevens die door meerdere toepassingen worden gebruikt) kunnen in een gedetailleerder onderverdeling van het record de belangrijkste gegevenselementen worden opgenomen.

Inpassing in het overzicht van de betreffende applicatie geeft het volgende beeld (zie figuur 3).



2	1	3	1
10-13	10-14	10-15	10-99
			X
			X
X	X		X
X	X		X
	X		X
		X	X
			X

Beschikbare verwerkingsfunctie

autorisatie

prog. nr.	benodigde authority	programma-omschrijving	sub-schema
01	10-10	Algemeen inquiry	08
02	10-11	Muteren artikelgegevens alg.	12
03	10-11/13/14	Muteren artikelprijzen	01
04	10-13/14	Factuurgegevens wijzigen	04
05	10-14	Facturen fiatteren	05
06	10-15	Muteren leveranciersgegevens	09
07	10-12	Goederenontvangst vastleggen	06
		Etc.	

Beschikbare gegevens

artikelomschrijvingen	artikelprijzen	leveranciers NAW	leveranciers overig	factuurgegevens	betaalgegevens	goederenontvangstinfo	sub-schema-nummers
R	R	R	R	R	R	R	08
R/W			R				12
R	R/W						01
	R			R/W			04
				R	R/W		05
		R/W	R/W				09
						R/W	06

Figuur 3. Overzicht bevoegdheden (authority profile).

Van de te onderzoeken applicatie is nu voldoende materiaal verzameld en gerangschikt om een oordeel over de ingebouwde functiescheidingen te kunnen vormen.
Een nadere analyse van de hiernaast gegeven informatie laten wij gaarne aan de lezer over.

B. Informatiebronnen

Waar komt de informatie voor het samenstellen van het overzicht vandaan.

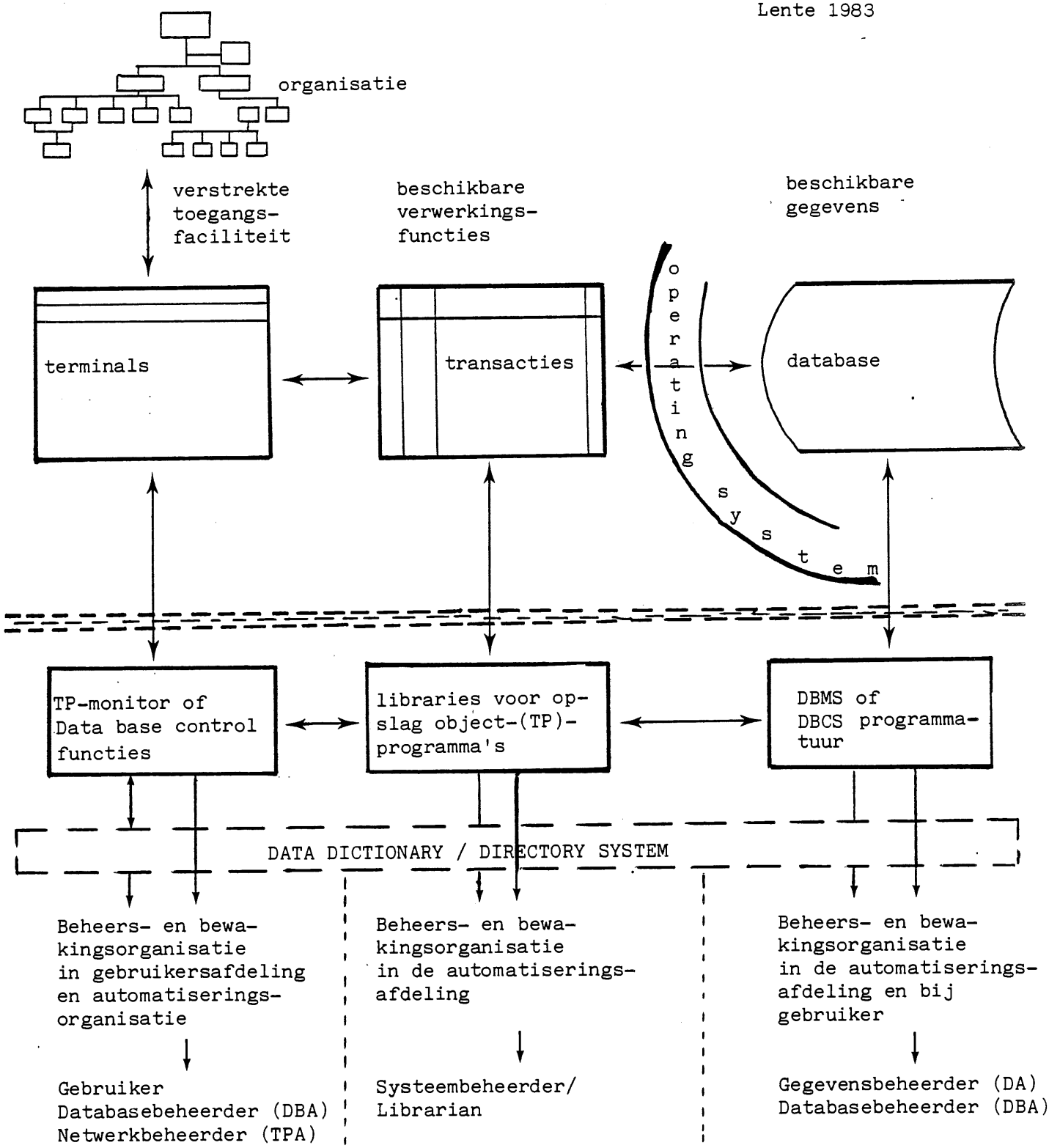
- Idealiter uit de systeemdocumentatie die bij de betreffende applicatie behoort. Deze documentatie geeft het zuiverste beeld van de opzet van de maatregelen van interne controle. Het is bovendien een gebruikersboek, waardoor de gebruiker zelf kan nagaan of een en ander volgens zijn aanwijzingen is opgezet. Wanneer bovendien een goede procedure voor wijzigingen van dit zogenaamde "authority profile" bestaat zal de accountant aan de hand van de wijzigingsformulieren, parafen, etc. kunnen nagaan of de bedoelde maatregelen van interne controle bestaan c.q. de procedures worden nageleefd. Helaas vinden we zelden een dergelijk gestructureerde omgeving, die het mogelijk maakt om met een geringe hoeveelheid arbeid het werkelijk in de computer aanwezige authority profile te toetsen aan de hand van de gebruikersdocumentatie.
- Soms is een datadictionary/directory systeem in gebruik waaruit de benodigde informatie kan worden verkregen.
  Ook hier gaat het om de vraag hoe sterk dit DD/DS verbonden is met de eindgebruiker van de applicatie enerzijds en met het actuele produktiesysteem anderzijds.
  Door bestudering van organisatie en procedures met betrekking tot het beheer van het DD/DS en de verantwoording die ten aanzien van dat beheer aan gebruikers wordt afgelegd, kan een indruk worden verkregen van de controle die een afzonderlijke gebruiker kan uitoefenen op "zijn" authority profile zoals dat in het actuele produktiesysteem op een zeker moment aanwezig is. Ook hier kan de accountant de inhoud van het DD/DS (de bedoeling) toetsen met het actuele produktiesysteem (de werkelijkheid).
  Een vervelend verschijnsel in de huidige DD/DS-en is dat zij doorgaans niet ingericht zijn om ermee te controleren. De hoeveelheid output (cross listings, authority listings, programma- en subschema-overzichten) die wordt verstrekt op grond van de vraag: wie mag wat met gegeven-X is veelal te overstelpend voor een snel, eenvoudig antwoord.
- Tenslotte is er de mogelijkheid dat de informatie slechts kan worden verkregen na raadpleging van tabellen van de TP-monitor en de generatie-overzichten van het DBMS.
  Die informatie moet dan worden afgestemd met de gebruiker om te zien of de automatiseringsafdeling heeft gehandeld conform de aanwijzingen van de gebruiker.

Dit is een omslachtige procedure en veelal is de informatie moeilijk leesbaar en slecht gestructureerd.
Ook de communicatie tussen automatiseringsafdeling en gebruiker zal in dit geval waarschijnlijk gebrekkig zijn.
De accountant zal zich moeten realiseren, dat hij hier in feite bezig is de "ist" situatie van een bepaald moment (namelijk van het tijdstip waarop de TP-monitor en het DBMS op de computer zijn geladen) te beoordelen.
Het is daarbij noodzakelijk, dat hij beschikt over de "soll"-positie zowel die van de gebruiker als die, welke hij zelf heeft opgesteld.

C. General controls

Al eerder merkten wij op dat de tot nu toe uitgevoerde activiteiten waren gericht op het verkrijgen van gegevens over de functiescheidingen met betrekking tot een bepaalde on-line applicatie voor de beoordeling van de opzet daarvan.

Uiteraard geeft de procedure en het verzamelen van gegevens al een indruk over de wijze waarop de gebruiker bij het automatiseringsgebeuren is betrokken, hoeveel controle hij kan of heeft kunnen uitoefenen op de activiteiten van de automatiseringsafdeling en hoe er in de automatiseringsafdeling wordt gewerkt.
Niettemin zal, om een gefundeerd oordeel te krijgen over het bestaan en de werking van de "general controls" verdergaand onderzoek nodig zijn.
In het volgende overzicht hebben wij de on-line applicatie geplaatst in zijn natuurlijke omgeving (zie figuur 4).



Figuur 4: De on-line applicatie in zijn natuurlijke omgeving.

Wij hebben in het overzicht de belangrijkste punten in de general controls aangegeven.
Voor wat betreft de automatiseringsorganisatie en de daarbij aanwezige functies en techniek valt uiteraard veel meer op te sommen dan waartoe wij ons hier beperkt hebben, doch voor die aspecten zullen inmiddels voldoende controlemiddelen en technieken bij de lezer bekend zijn.

Met welke diepgang het onderzoek van de general controls moet worden verricht, zal van geval tot geval verschillen.
Ook hier moet onderscheid worden aangebracht tussen een beoordelings- en een toetsingsfase.
Zoals al eerder opgemerkt is, zal in de procedure van het verzamelen en vastleggen van materiaal over de applicatie al een indruk ontstaan van de invloed die uitgaat van de general controls. Met behulp van checklists voor automatiseringsorganisaties kan deze indruk nader worden getoetst.
Het oordeel over de opzet en de werking van de general controls is tenslotte bepalend voor de frequentie waarmee controles ter plaatse zullen worden uitgevoerd (bijvoorbeeld vergelijkingen van in de computer aanwezige authority profiles, actuele programma's, subschema's e.d. aan de hand van de documentatie).

V Afronding

Er zijn nog vele andere facetten die samenhangen met gebruik en controle van on-line applicaties. Wij hebben deze aspecten bewust weggelaten omdat het artikel dan nog langer zou worden dan nu al het geval is. Voor de geïnteresseerde lezer geven wij een korte opsomming van de belangrijkste aspecten met een korte toelichting.

- Testen.
  Hoe test de gebruiker de on-line applicatie; kan een accountant er nog een testset op nahouden, die hem toereikende informatie geeft?
  - Gebruikerstesten zouden in "batch-mode" moeten worden uitgevoerd om een goede vastlegging te krijgen van hetgeen getest is en hoe.
  - De testset van de accountant is niet meer bruikbaar. Het mooiste zou zijn, wanneer er een retrievalpakket zou worden meegeleverd door de makers van het DBMS waaruit eenzelfde overzicht kan worden gehaald, als wij in dit artikel hebben opgebouwd. Dit pakket zou dan informatie moeten krijgen uit het "live-system".
- Rechtstreekse ingangen.
  Niet elke databasebenadering loopt via het bewakingssysteem dat voor "normale" gebruikers is opgezet. Database-administrator, operators, systeemprogrammeurs kunnen in noodgevallen (reparatie database-structuren) rechtstreeks gebruikersdata benaderen.
  Procedures voor gebruik van deze commands moeten aanwezig zijn, evenals toezicht en verantwoording achteraf.
- Batchprogramma's.
  Bedacht moet worden, dat een batchprogramma niet via de TP-monitor/ gebruikersbeeldschermen wordt gestart. De passwords voor onder andere het openen van de database moeten niettemin worden opgenomen. In het ergste geval zijn deze passwords in het batchprogramma opgenomen waardoor iedereen die de programmasource te pakken kan krijgen, kan beschikken over passwords van database, subschema's, etc.

- Menu-security.
  We hebben het niet gehad over een belangrijk additioneel middel om gebruikers beperkingen op te leggen met betrekking tot het starten van verwerkingsfuncties, namelijk het gebruik van beeldscherm-menu's.
  Door een goede opzet van de menu's wordt een gebruiker gedwongen een bepaald (verwerkings-)pad te volgen dat speciaal voor hem is gemaakt. Een pad komt beschikbaar wanneer een bijbehorende gebruikersidentificatie en password bekend wordt gemaakt aan het systeem.
  Helaas beschikken vele systemen daarbij ook over mogelijkheden om uit het menu te "springen".
  Op de menu-security kan zodoende niet altijd onvoorwaardelijk worden vertrouwd; gebruikers die à la carte wensen te werken (al dan niet met toestemming) dienen ook in dat geval met voldoende beveiligingsmaatregelen te worden geconfronteerd.

Samenvatting

In grote trekken is in dit artikel het verschijnsel on-line systemen belicht vanuit de behoefte hiervoor een adequate controlebenadering te vinden. Voor deze benadering hebben wij - na enige beschouwende paragrafen over techniek en algemene controleproblematiek - gekozen voor een stapsgewijze beschrijving van de belangrijkste werkzaamheden die zullen moeten worden uitgevoerd.
De aanpak van de accountantscontrole dient daarbij zoveel mogelijk te worden afgestemd op de gebruikersbenadering. Uiteraard niet zo vanzelfsprekend als dat hier wordt samengevat; een beoordeling van die gebruikersaanpak met het oog op verwerkingsaard en de belangen van collega-database gebruikers is noodzakelijk.
Uitgaande van een systeemgerichte gebruikersbenadering onderzochten wij via transactie-analyse de aanwezige functiescheiding in de on-line applicatie. De ervaringen uit dit onderzoek en de wijze waarop de gebruiker vanuit de automatiseringsomgeving wordt geïnformeerd bepalen de omvang en de diepgang van het onderzoek naar bestaan en werking van de "general controls".

Dit artikel zal mogelijk nog een aantal vragen van praktische aard oproepen. In onze cursus "Accountantscontrole bij Geïntegreerde Gegevensverwerking" (GGV) worden de verschillende facetten meer diepgaand behandeld. In de rubriek Onderwijs in dit blad staat aangegeven hoe u onze brochure kunt aanvragen.

(Met toestemming van Marten Toonder Studio's hebben wij uit twee stripverhalen overdrukken in dit artikel opgenomen.
De 1e strip komt uit "De Weetmuts", een schitterend relaas over de lijdensweg van een Heer die alles weet.
De 2e en 3e strip zijn overgenomen uit "De Transmieter", een verhaal waarin Bommel een zeer bijzondere terminal in bezit krijgt en in zijn goedheid daarmee de computersystemen van de gemeente Rommeldam onbedoeld ontregelt.)

COMPACT

Lente 1983

Beheersing, beveiliging en controle van het IBM Systeem/38

door A.H.C. Koedijk

(Dit artikel is gebaseerd op de presentaties die door de schrijver zijn gegeven op de 13th Conference on Computer Audit, Control and Security, Chicago, 9-13 mei 1983.)

1. Introductie

De architectuur van het IBM Systeem/38 biedt nieuwe mogelijkheden op het gebied van beheersing, beveiliging en controle. Voorwaarde is evenwel, dat betrokkenen een goed begrip hebben van de wijze waarop parallelen kunnen worden getrokken tussen algemene beheersbaarheidsconcepten en de bijzondere S/38-filosofie.

Na een korte beschrijving van de beheersbaarheidsconcepten in hoofdstuk 2, worden in de hoofdstukken 3, 4 en 5 de architectuur en de beheersings- en beveiligingsstructuur van de S/38 behandeld. In hoofdstuk 6 worden vervolgens de parallelen getrokken tussen de automatiserings- en bedrijfsfuncties en de technische S/38 computeromgeving; dit wordt gedaan door middel van een stapsgewijze beschrijving van de wijze waarop de beheersbare conceptuele organisatie ook in de computer kan worden geëffectueerd. In hoofdstuk 7 worden tenslotte de controlemogelijkheden belicht; eerst een stapsgewijze beschrijving van een (door geautomatiseerde procedures ondersteund) onderzoek naar de wijze waarop van de mogelijkheden van de S/38 gebruik wordt gemaakt, vervolgens de S/38 bij het werken met "conventionele" controleprogrammatuur.

2. Conceptuele bedrijfsorganisatie: een raamwerk voor beheersing en controle

Introductie

In het algemeen is in een S/38-omgeving sprake van een door verschillende gebruikers gemeenschappelijk benutte computer. Bovendien zal er een toenemend gemeenschappelijk gebruik zijn van de in databases opgeslagen gegevens.
Het ligt voor de hand dat in een dergelijke situatie enige problemen met betrekking tot de beheersbaarheid ontstaan.
Wanneer een computersysteem moet worden beoordeeld op de mogelijkheden terzake van beheersbaarheid, is er behoefte aan een raamwerk in de vorm van een modelorganisatie, zodat afstand kan worden genomen van in de praktijk aanwezige verschillen.
In dit hoofdstuk wordt een dergelijk raamwerk besproken.

Conceptuele bedrijfsorganisatie

Het gebruik van een computer voor de gegevensverwerking van een organisatie leidt tot een behoefte aan specifieke kennis en ervaring. Deze kennis en ervaring zijn relatief schaars. Teneinde optimaal profijt te kunnen trekken, zullen deze kennis en ervaring worden geconcentreerd in afzonderlijke functies. De samenwerking tussen de klassieke bedrijfsfuncties en deze verbijzonderde automatiseringsfuncties wordt gekenmerkt door delegatie.

Sterk gesimplificeerd is er in principe samenwerking tussen de bedrijfsfuncties en de automatiseringsfuncties Systeemontwikkeling (met name Programmering) en Verwerking. Er worden programma's geschreven, gecontroleerd en geaccepteerd volgens geldende procedures. Geautomatiseerde systemen worden, na ontwikkeling door Programmering, aan de bedrijfsfunctie beschikbaar gesteld ter acceptatie. Na acceptatie gaat het systeem over naar Verwerking voor bewaring en uitvoering.

In de situatie waarin bedrijfsfuncties identieke gegevens gebruiken, zal (ondersteund door database-technieken) een tweede vorm van samenwerking ontstaan: de verschillende bedrijfsfuncties zullen gezamenlijk gebruik gaan maken van dezelfde fysieke gegevens. Hieruit vloeit een beheersingsvraagstuk voort, namelijk de toekenning van verantwoordelijkheden ten aanzien van de volledigheid, juistheid en actualiteit van deze gegevens. Beheersing en coördinatie moeten worden uitgeoefend door een afzonderlijke functie: Gegevensbeheer (data administration) (III)*). Om deze functie goed te kunnen uitoefenen heeft Gegevensbeheer in het algemeen behoefte aan een hulpmiddel voor de registratie van gegevens (naam, definitie, eigenschappen) over gegevens en van gegevens over het gebruik van gegevens (wie heeft welke bevoegdheden met betrekking tot welke gegevens en wanneer); dit hulpmiddel staat bekend als data dictionary. De beheersbaarheid kan worden verbeterd, als Gegevensbeheer programmeurs kan dwingen tot het gebruik van bestanden die volgens algemeen geldende definities zijn gecreëerd.

De scheiding tussen de verschillende functies kan slechts bijdragen tot beheersing van het gegevensgebruik indien het computergebruik voor elke functie kan worden beperkt tot een groep bepaalde, nauw omschreven programma- en gegevenssoorten.
Zo een door een bepaalde functie te gebruiken groep programma- en gegevenssoorten wordt aangeduid als domein of omgeving.
Er is behoefte aan verschillende omgevingen voor:
1. Bedrijfsfuncties met operationele toepassingssystemen.
2. Programmering met toepassingen in ontwikkeling.
3. Verwerking.
4. Gegevensbeheer.

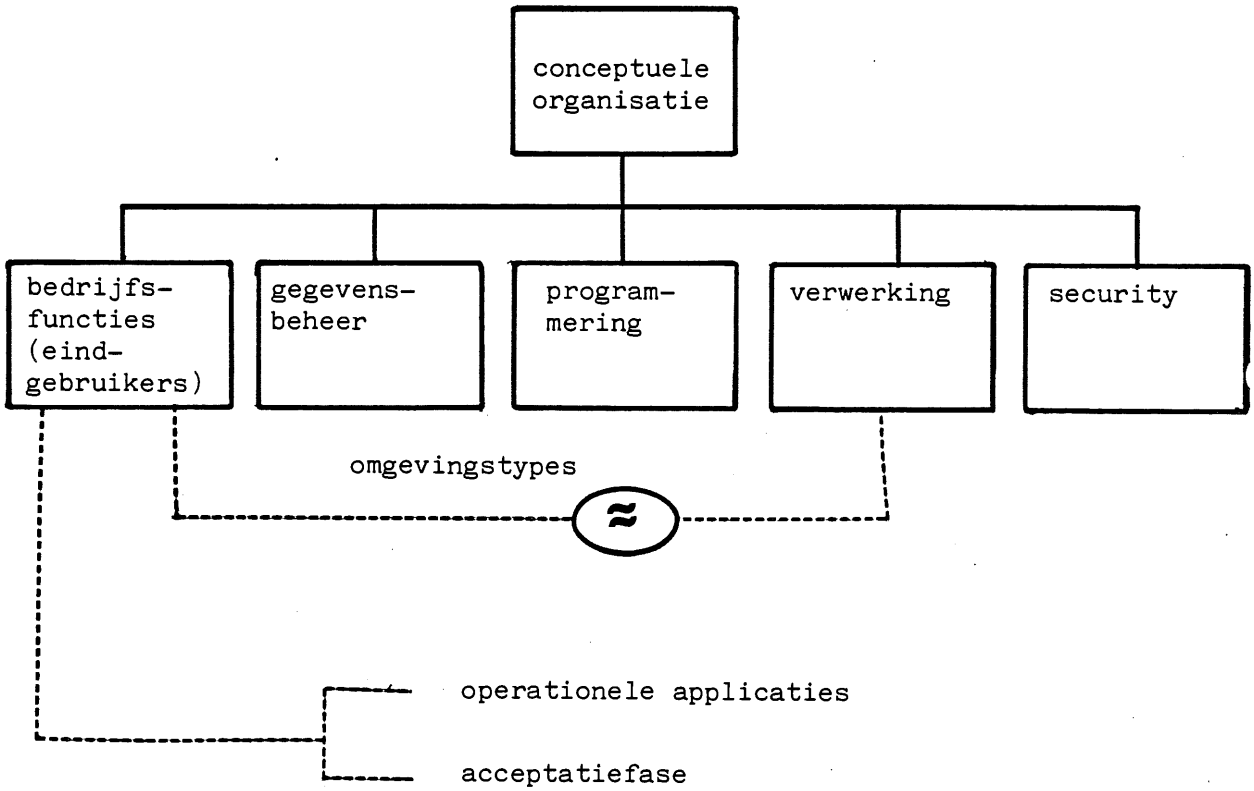
In een situatie met een hoge graad van interactieve computerprocessen, hetgeen in de situatie met een S/38 veelal het geval zal zijn, valt de Verwerkingsfunctie goeddeels weg. De bedrijfsfuncties zullen de produktie-activiteiten in belangrijke mate zelf regelen.

*) Romeinse cijfers verwijzen naar de literatuuropgave aan het einde van het artikel.

Ten aanzien van de gewenste omgevingen geldt, dat geen der functies in staat mag zijn ongevraagd het domein van een ander te "betreden". Hierdoor is er behoefte aan nog een functie, die, refererend aan de S/38 terminologie (security officer), Security zal worden genoemd. (Een betere naam voor deze functie zou zijn Bevoegdhedenbeheer.) Security creëert de omgevingen per functie. Security draagt zorg voor de overdracht van systemen (programma's en bijbehorende bestanden of databases) van de ene omgeving naar de andere. Kritiek punt in de samenwerkingen is de systeemacceptatiefase en de overdracht van geaccepteerde systemen naar een Verwerkingsomgeving. Gedurende de acceptatiefase kan de bedrijfsfunctie niet ook maar enige controle overlaten aan Programmering. De Programmeringsomgeving is derhalve ongeschikt. Ook de Verwerkingsomgevingen zijn niet geschikt voor de acceptatiefase: mogelijk instabiele systemen zouden de werkelijke bedrijfsgegevens ongewenst kunnen beïnvloeden. Een speciale omgeving voor de acceptatiefase is derhalve nodig.

Samenvatting

Noodzakelijke functiescheidingen in de organisatie moeten kunnen worden doorgetrokken tot in het computersysteem:



De sleutelvraag is nu, of en hoe de mogelijkheden die de S/38 biedt, op deze organisatorische functiegebieden kunnen worden afgestemd.

3. Systeem/38

Architectuur

Het gemeenschappelijk gebruik van een computersysteem heeft tot gevolg dat:
- gegevens van verschillende bedrijfsfuncties zich in één en dezelfde machine bevinden;
- verwerkingsprocessen ten behoeve van verschillende gebruikers gelijktijdig plaatsvinden.

Programma's mogen elkaar en elkaars gegevens niet beïnvloeden.
Het hoofdprobleem ligt in het gemeenschappelijk gebruik van geheugens. Er is behoefte aan geheugenbescherming.

Geheugenbescherming wordt doorgaans gerealiseerd door het toekennen van sleutels aan processen. Deze sleutels moeten passen op sloten, die worden geïnstalleerd op geheugendelen die aan het proces zijn toegekend. Het toekennen van sleutels en installeren van sloten gebeurt gewoonlijk door een overkoepelend proces, het operating system, dat daartoe de beschikking heeft over specifieke instructies. Om deze instructies te kunnen uitvoeren, moet de machine in de "privileged state" zijn. Deze status kan ontstaan ten gevolge van een interrupt. In deze situatie is het gehele geheugen toegankelijk voor het operating system.
Een probleem hierbij is, hoe kan worden voorkomen dat "gewone" gebruikers (toepassingsprogrammeurs) hun proces in "privileged state" kunnen laten komen. In vele gevallen biedt de machine-interface (gewoonlijk een assembler) in principe deze mogelijkheid.

Een andere methode om te voorkomen dat processen elkaar beïnvloeden is het gebruik van "capabilities". Een capability omvat een door de machine toegekende unieke naam per programma, bestand of welke entiteit ("object") in de machine dan ook, alsmede toegangsrechten (I, II)*). De entiteiten zijn alleen adresseerbaar door middel van de naam. De naam wordt opgeslagen in beschermd geheugen en kan niet door gebruikers worden gemanipuleerd. Elke poging om een naam, die in wezen een "pointer" is, te wijzigen, moet leiden tot vernietiging van die pointer.
Deze principes zijn toegepast in het Systeem/38. Ze worden uitgevoerd door hardware en/of microcode, en niet door een uit in wezen "gewone" programma's bestaand operating system.

S/38-basisconcepten

Het Systeem/38 is een op objecten gebaseerd systeem, waarin de adressering is gebaseerd op capabilities (namen). Alle entiteiten in het systeem worden gerepresenteerd in de vorm van objecten, bijvoorbeeld een reeks bij elkaar behorende instructies (object type "programma") of een reeks adresseerbare gegevens (object type "bestand"). De start- en eindadressen van een object worden door de machine toegekend en zijn geldig gedurende het bestaan van het object.

*) Literatuuropgave.

Een object wordt gedefinieerd als een benoemde entiteit, die verder wordt beschreven door de functies en bewerkingen die met of op het object kunnen worden uitgevoerd. (Andere namen hiervoor zijn "extended data type" en "abstract data type".)
Op het hoogste niveau zijn er twee types: de systeemobjecten (ondersteund door de machine) en de CPF-objecten (ondersteund door het CPF, Control Program Facility, het operating system van de S/38; het CPF bestaat in wezen uit een aantal objecten). De systeemobjecten worden in dit artikel buiten beschouwing gelaten.
Het CPF ondersteunt 23 (release 4.1) verschillende CPF-object types. Voor elk object type bestaan commando's om objecten te creëren, te onderhouden of te gebruiken.
De CPF-objecten zijn beschreven in bijlage 1 (bron: IBM manual).

Programmeurs zien geen verschil tussen intern en extern geheugen. De machine biedt één geheugen, noodzakelijk voor de realisering van capability adressing.

Van het CPF is geen source-versie beschikbaar voor gebruikers. IBM verschaft slechts een laadbaar operating system in microcode.
Ook is er geen machine-interface beschikbaar. Het laagste niveau van interface is de user interface: de CPF Command Language (CL).

4. Beheersings- en beveiligingsstructuur S/38

User-profiles, menu's, passwords

User-profiles zijn verbonden aan een password voor de aankoppeling en zijn zelf ook beschermd door een password, namelijk dat van de "security officer" (een specifiek user-profile in de S/38).
In elk user-profile kan een initieel programma worden gespecificeerd, dat normaliter automatisch wordt opgestart na aankoppeling door de desbetreffende gebruiker. Dit heeft de intentie de gebruiker in het keurslijf van een menu te dwingen, waarmee hij kan worden beperkt in zijn toegang tot programma's en bestanden.
Menu's behoren echter niet tot de ontworpen beveiligingsstructuur van de S/38. Ze ondersteunen de gebruikersvriendelijkheid.
Om verschillende redenen moet de toepassing van menu's worden aanbevolen, maar de beveiliging moet (anders dan in vele andere situaties, bij voorbeeld met een Systeem/34) hierop niet worden gebaseerd.

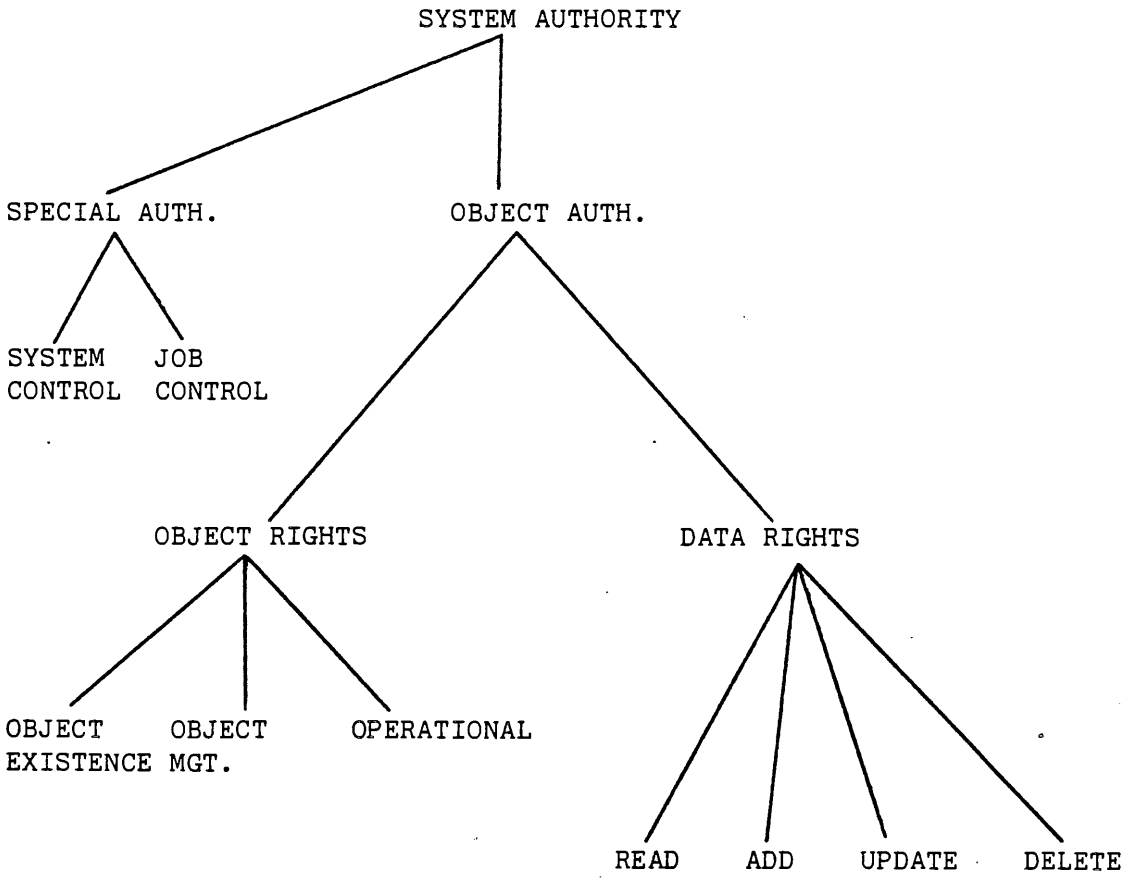
In het systeem bevindt zich standaard een aantal user-profiles:
- security officer (QSECOFR)
- programmer (QPGMR)
- workstation user (QUSER)
- system operator (QSYSOPR)
- IBM programming service representative (QPSR)
- IBM system engineer (QCE).

Al deze profiles, behalve dat van de security officer, bevatten de naam van een initieel programma. Ze zijn eveneens verbonden aan een initieel password.
Spoedig na installatie van een S/38 dient de security officer deze initiële passwords te wijzigen!

De user-profiles worden beheerd door de security officer, die ook het beheer over de passwords voert. Het beheer van de passwords kan bij de gebruikers zelve worden gelegd, doch de security officer behoudt altijd toegang tot de passwords en derhalve tot alle objecten in het systeem.
De security officer heeft dus toegang (en bevoegdheden) tot alle objecten in het systeem. Dit is een direct gevolg van de in het CPF gerealiseerde hiërarchische beveiligingsstructuur: de "man at the top" heeft nogal wat macht.
De S/38 structuur biedt de mogelijkheid security officer bevoegdheden geheel of ten dele aan andere user-profiles toe te kennen. Dit is in het huidige CPF echter niet opgenomen.
Op dit moment kan de verantwoordelijkheid voor de security officer functie in twee handen worden gelegd door het security officer password in een badge vast te leggen, dat onder dubbele versluiting wordt bewaard (hiertoe dient een badge-reader aan een werkstation te worden gekoppeld), of - eenvoudiger - door het password van de security officer in tweeën te delen, waarbij elk deel door een ander wordt gekend en beheerd.

CPF beveiligingsstructuur

De beveiliging in het Systeem/38 is geregeld door passwordbescherming op de aankoppeling van gebruikers, specifieke toekenning van bevoegdheden met betrekking tot besturingsoperaties en specifieke toekenning van bevoegdheden om objecten (programma's, bestanden, e.d.) te beheren of te gebruiken.
De structuur kan schematisch als volgt worden weergegeven:



Special authority

Indien aan een gebruiker special authority wordt toegekend, wordt dit vastgelegd in zijn user-profile. Er zijn twee soorten special authority:

- save system: save/restore-rechten ten aanzien van objecten;
- job control: rechten ten aanzien van jobqueues, jobs, outputqueues, bestanden in outputqueues.

Deze rechten worden doorgaans alleen aan de operator toegekend, waarbij bedacht moet worden, dat gebruikers vergelijkbare rechten bezitten ten aanzien van de objecten die ze in eigendom hebben.

Een object bestaat uit twee delen: een "description" en een "data part" (de feitelijke inhoud van het object, bijvoorbeeld de records in een file). Bij save wordt het gehele object gekopieerd. Bij restore wordt alleen het data part teruggeplaatst, tenzij het object tussen de save en restore operaties werd uitgewist (delete). In dat geval wordt het gehele object teruggeplaatst.
Als een object door middel van restore wordt teruggeplaatst, kijkt het systeem of de in het object vermelde eigenaar overeenstemt met het in het desbetreffende user-profile vastgelegde eigenaarschap (zie ook de volgende paragraaf). Als dit niet overeenstemt wordt automatisch de security officer als de eigenaar aangemerkt.

Object authority

Een gebruiker die een object creëert, is hiervan de eigenaar en heeft alle bevoegdheden ten aanzien van dat object. De eigenaar kan echter rechten toekennen aan andere gebruikers, bijvoorbeeld op het gebruik van gegevens in bestanden.
Het eigenaarschap wordt vastgelegd in het description-deel van het object. Daarnaast bevat een user-profile een lijst van de objecten waarvan de betreffende gebruiker eigenaar is.

Object authority omvat twee groepen rechten:
rechten op het object als geheel (object rights), bijvoorbeeld een bestand en rechten op het data part van het object (data rights), bijvoorbeeld ten aanzien van het object type bestand: de records in een bepaald bestand.

Objects rights

- existence: delete, save, free storage, restore, overdragen eigendom;
- management: verplaatsen, herbenoemen, bevoegdheden toekennen aan/herroepen van andere gebruikers;
- operational: het kunnen lezen van de beschrijving van het object; het object mogen gebruiken. (Deze rechten variëren per object type; ze kunnen tevens enige data rights omvatten).

Indien het eigenaarschap wordt overgedragen, verdwijnen de hierbij behorende rechten niet automatisch uit het user-profile van de "oude" eigenaar. Deze moeten uitdrukkelijk worden herroepen ("revoke") door de nieuwe eigenaar.

Data rights

- read: het mogen lezen van het data-part, bijvoorbeeld de records in een file;
- update: het mogen wijzigen van de inhoud van het data-part;
- add: het mogen toevoegen aan het data-part;
- delete: het mogen verwijderen uit het data-part.

Zoals gezegd heeft de eigenaar volledige bevoegdheid ten aanzien van zijn objecten. Hierna wordt aangegeven hoe rechten aan andere gebruikers kunnen worden toegekend ("grant").

Toekennen van rechten

Zowel object rights als data rights kunnen aan andere gebruikers worden toegekend. Dit kan expliciet aan individuele gebruikers worden gedaan (private), of aan alle gebruikers (public).

Private rights worden vastgelegd in de desbetreffende user-profiles. Ze worden toegekend door de Grant Object Authority of Grant User Authority commands. Ze kunnen worden herroepen door het Revoke Object Authority command.

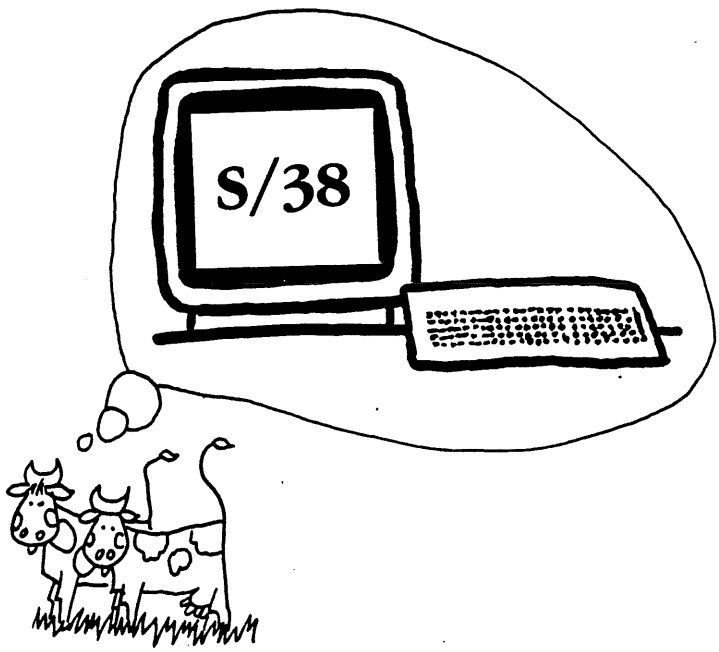
De volgende tabel uit het IBM-manual geeft aan welke data rights automatisch zijn vervat (aangegeven door een "O") in de toekenning van (private) operational rights.

Object Type	Data Rights			
	Read	Add	Update	Delete
Class	O	O	O	O
Command	O	O	O	O
Control unit description	O	O	O	O
Data area	O	O		O
Device description	O	O	O	O
Edit description	O	O	O	O
File				
Forms control table	O	O	O	O
Job description	O	O	O	O
Job queue				
Journal				
Journal receiver				
Library	O			
Line description	O	O	O	O
Message file				
Message queue				
Output queue				
Program		O	O	O
Print image	O	O	O	O
Session description	O	O	O	O
Subsystem description	O	O	O	O
Table	O	O	O	O
User profile				

De toekenning van "public" rechten kan gebeuren bij creatie van het object, of door middel van het Grant Object Authority command. Public authority wordt vastgelegd in de object descriptions.
Public authority kan als volgt worden gespecificeerd:

- normal: alle gebruikers krijgen "normale" bevoegdheden ten aanzien van het gebruik van het object; dit is een combinatie van operational authority en enige of alle data rights, afhankelijk van het object type (zie tabel hierna);
- none: alleen de eigenaar, de security officer en gebruikers die expliciet rechten kregen toegekend (private) kunnen het object gebruiken;
- all: elke gebruiker kan het object als ware hij de eigenaar (dus ook delete!) gebruiken.

Object existence rights en object management rights worden nooit toegekend als onderdeel van "normal public authority".



S/38: een gebruikersvriendelijke computer

De volgende tabel uit het IBM-manual geeft weer welke rechten worden toegekend bij "normal public authority" (aangegeven door een "N"):

Object Type	Object Rights	Data Rights			
	Operational	Read	Add	Update	Delete
Class	N	N	N	N	N
Command	N	N	N	N	N
Control unit description	N	N	N	N	N
Data area	N	N	N	N	N
Device description	N	N	N	N	N
Edit description	N	N	N	N	N
File (see note)	N	N	N	N	N
Forms control tabel	N	N	N	N	N
Job description	N	N	N	N	N
Job queue	N	N	N		
Journal	N	N	N	N	
Journal receiver	N	N			
Library	N	N	N	N	N
Line description	N	N	N	N	N
Message file	N	N			
Message queue	N	N	N		N
Output queue	N	N	N		
Program	N	N	N	N	N
Print image	N	N	N	N	N
Session description	N	N	N	N	N
Subsystem description	N	N	N	N	N
Table	N	N	N	N	N
User profile	N				

Noot: Data rights kunnen niet worden gespecificeerd voor logical files.

Om een CPF-object te kunnen gebruiken, moet een gebruiker zowel bevoegdheden bezitten ten aanzien van het object als ten aanzien van de bibliotheek waarin het object zich bevindt. Bij creatie van het object kan worden opgegeven in welke bibliotheek het moet worden geplaatst (de General Purpose Library, standaard in het CPF, is default, hetgeen wil zeggen, dat deze bibliotheek wordt gebruikt tenzij een andere wordt gespecificeerd), behalve voor de vanuit beveiligingsoogmerk belangrijkste object typen user-profile en bibliotheek, alsmede enige hardware beschrijvingen. Deze objecten worden automatisch in de systeembibliotheek QSYS, geplaatst.

De naam van een object bestaat uit twee delen ("qualified name"): de objectnaam en de bibliotheeknaam. Deze qualified names kunnen worden benut om de verschillende gebruikersdomeinen te creëren en de overdracht van objecten van de ene omgeving naar de andere efficiënt te regelen (zie hoofdstuk 6).

5. Ondersteuning voor Gegevensbeheer en Programmering

Programmering

Het CPF verschaft een uitgebreide ondersteuning voor de programmeurs in de vorm van een Source Entry Utility om interactief programma's te schrijven in RPG III, COBOL of de CPF Command Language (CL), een Data File Utility (DFU) ten behoeve van data entry en updaten van bestanden, een Query-faciliteit en een Screen Design Aid (SDA) voor het creëren van scherm layouts en menuprogramma's.

RPG III is gebaseerd op z'n voorgangers RPG en RPG II, maar kent enige uitbreidingen. In het bijzonder is de Data Description Specification (DDS)faciliteit van belang. Hiermee kunnen alle databases in het systeem worden beschreven, los van de toepassingsprogrammatuur.
Sources van RPG III-programma's en van DDS-gegevensbeschrijvingen worden gebruikt door CPF Commands die uitvoerbare programma's en fysieke of logische bestanden creëren.

Gegevensbeheer

RPG III biedt de mogelijkheid om files binnen een programma te beschrijven (om conversie van programma's in RPG II te vergemakkelijken), of om afzonderlijk (extern, door middel van DDS) gedefinieerde bestanden te gebruiken. In het eerste geval wordt gesproken over "program defined"bestanden, in het laatste geval over "externally defined"-bestanden.
Bij het definiëren van een bestand kan worden gerefereerd naar elders beschreven velden. Dit verschaft de mogelijkheid om centraal een zogenaamde "field reference file" (FRF) te onderhouden, waarin alle velddefinities en formaatbeschrijvingen worden opgenomen. De FRF vormt een belangrijk stuk gereedschap voor de Gegevensbeheer functie. De FRF is een gewone fysieke file, die echter niet wordt gecreëerd met als doel "echte" gegevens te herbergen; het data part wordt gewoonlijk leeg gelaten. Alleen het description deel wordt benut: hierin zit één (grote) recordbeschrijving met daarin alle waar dan ook gebruikte velden; hiernaar kan worden gerefereerd als "echte" bestanden worden beschreven en gecreëerd.

Bij het beschrijven en creëren van bestanden kan echter naar elk ander bestand worden verwezen; bovendien kunnen definities ook in de beschrijving zelf worden opgenomen. De overeenstemming tussen de FRF en de echte bestanden moet derhalve door procedures worden ondersteund, hetgeen een taak vormt van Gegevensbeheer. Gegevensbeheer zal hierin moeten samenwerken met de security officer.

Een zeer sterke eigenschap van de S/38 is de mogelijkheid om op elk gewenst moment de objectbeschrijvingen via een display zichtbaar te maken. De informatie die via een display wordt verstrekt, is dezelfde informatie waarmee het systeem werkt ten behoeve van de verwerking (in wezen is dit een voorbeeld van een "active data dictionary"). Deze eigenschap is van bijzondere betekenis voor controledoeleinden gezien de één op één relatie die bestaat tussen ieder object en de daarbij behorende beschrijving. Deze relatie is niet te doorbreken.

Ook zijn er commands om de volgende informatie zichtbaar te maken:
- welke files worden gebruikt door een bepaald programma;
- welke fysieke files worden benaderd via een bepaald logisch bestand (een logisch bestand vormt ware een "user view" op gegevens; de gegevens in een logisch record kunnen een subset vormen van het fysieke record; het toegangspad - volgorde - kan per gebruiker verschillen);
- via welke logische files wordt een bepaald fysiek bestand benaderd.

6. Realisatie van de conceptuele organisatie met het CPF

In hoofdstuk 2 werden de volgende functies onderscheiden:
- Bedrijfsfuncties (eindgebruikers):
  - produktie
  - acceptatietestfase
- Programmering
- Gegevensbeheer
- Security.

De standaard CPF object typen bieden goede mogelijkheden tot het realiseren van de noodzakelijke gescheiden omgevingen.

De vanuit het gezichtspunt van beveiliging voornaamste object types zijn programma's en bestanden.

Enkele kerndoelstellingen zijn:
- Gegevensbeheer wil er zeker van zijn dat in operationele systemen de regels met betrekking tot het gebruik van gegevens worden nageleefd;
- Eindgebruikers willen er zeker van zijn, dat geaccepteerde systemen ongewijzigd blijven;
- Security wil dat de afzonderlijke omgevingen in stand worden gehouden.

Twee principes kunnen worden toegepast:
- om een object te kunnen gebruiken, moet de gebruiker de vereiste bevoegdheden hebben ten aanzien van dat object alsmede tenminste operationele bevoegdheid ten aanzien van de library waarin het object zich bevindt;
- overdrachten van de ene omgeving naar de andere worden beheerst door Security.

Voorbeeld van de realisatie van een beheersings- en beveiligingssysteem

1. Security creëert bibliotheken van 4 typen: Gegevensbeheer, Programmering, Acceptatie, Eindgebruikers-produktie.

2. Teneinde alle bibliotheken te kennen, reserveert Security het Create Library command voor zichzelf; ten gevolge daarvan is Security eigenaar van alle bibliotheken.

3. Teneinde op de hoogte te zijn van alle bevoegdheden van alle gebruikers zal Security in principe slechts operationele bevoegdheid ten aanzien van bibliotheken toekennen aan gebruikers. Operationele bevoegdheid impliceert het data right "read".

4. Gebruikers krijgen voor de bibliotheken binnen hun eigen omgeving ook de data rights "add" en "delete".

5. Databases worden alleen als extern beschreven bestand gecreëerd:
   5.1 Gegevensbeheer creëert in zijn bibliotheek een field reference file (FRF); elk gegevenselement wordt daarin één maal beschreven.
   5.2 Voor iedere database wordt, refererend naar de FRF, een sourcefile gecreëerd. Deze sourcefiles bevatten met RPG-source programma's vergelijkbare bestandsdefinities die worden gebruikt bij de creatie - vergelijkbaar met compileren - van de "echte" bestanden.
   5.3 Vanuit deze sourcefile wordt de fysieke file gecreëerd.
   5.4 Eveneens via sourcefiles worden over de fysieke files logical files gedefinieerd.
   5.5 Beide filetypen worden gecreëerd met de opties LVLCHK(*YES) en PUBAUT(*NONE). Levelcheck (LVLCHK) heeft tot gevolg dat, telkens wanneer de betreffende file wordt verbonden aan een actief programma, wordt gecontroleerd of de file-definitie nog hetzelfde is als ten tijde van de creatie van het programma. PUBAUT is de public authority parameter.
   5.6 Beide filetypen moeten, tijdens de ontwikkelingsfase, beschikbaar zijn voor de programmeur; Gegevensbeheer plaatst de files daartoe tijdens creatie in de programmeursbibliotheek. Hiertoe moet Gegevensbeheer operationele en add bevoegdheden hebben ten aanzien van deze bibliotheken. Gegevensbeheer creëert de databases en is hiervan derhalve eigenaar.

6. Programmeurs ontwikkelen sourceprogramma's in database sourcefiles in hun eigen bibliotheken.

7. Uitvoerbare programma's worden door de programmeur gecreëerd vanuit de sourcefiles met het create RPG/COBOL/CL-programma command. Dit geschiedt met de optie user-profile "*OWNER". De creator moet operationele bevoegdheid ten aanzien van alle gerefereerde objecten (in het bijzonder de te benaderen bestanden) hebben. Deze bevoegdheid alsmede de voor het testen benodigde data rights, wordt door Gegevensbeheer toegekend.

8. Indien de programma's gereed zijn voor acceptatie, brengt Security de programma's over naar een Acceptatiebibliotheek. De namen van de objecten blijven gelijk voor wat het eerste deel betreft, de qualifier (de library naam) maakt de naam als geheel uniek. Ook alle objecten die in de programma's worden gebruikt, moeten in deze overdracht zijn betrokken:
   8.1 Security stelt vast welke bestanden door de programma's worden gebruikt door middel van het DSPPGMREF command (display program references).
   8.2 Gegevensbeheer controleert deze informatie en zet de bestanden over naar de Acceptatiebibliotheek. Hiertoe kent Security op deze bibliotheek operationele en add bevoegdheid toe aan Gegevensbeheer.
   8.3 Gegevensbeheer maakt de bestanden schoon, zodat hierin de testgegevens kunnen worden opgebouwd (CLRFM command);
   8.4 Doordat de programma's werden gecreëerd met de optie user-profile "*OWNER" (zie stap 7), vindt uitvoering van de programma's plaats met de bevoegdheden uit zowel het user-profile van de eindgebruiker als die uit het profile van de eigenaar (de programmeur); hierdoor heeft de eindgebruiker de bevoegdheid om de betrokken bestanden te benaderen "geadopteerd" van de programmeur.
   8.5 De eigenaar van de programma's, de programmeur, heeft geen bevoegdheden ten aanzien van de Acceptatiebibliotheek: hij kan de acceptatietest niet beïnvloeden.
   8.6 De optie LVLCHK(*YES), zie stap 5.5, die bij creatie van de bestanden werd gehanteerd, draagt er zorg voor dat de gegevensdefinities zoals die naar het programma werden gecopieerd, overeenstemmen met de definities in de extern gedefinieerde file zelf (in het description deel). Level checking wordt bij elke "open" van het bestand uitgevoerd.

9. Na formele acceptatie worden de programma's en bestanden overgezet naar de eindgebruikers produktiebibliotheken. Deze procedure is gelijk aan die onder 8.

10. Indien wijzigingen moeten worden aangebracht, kan de procedure op gelijke wijze in omgekeerde richting worden uitgevoerd.
    Bij wijzigingen van een database echter, zal de betreffende fysieke file operationeel moeten blijven. De fysieke file zal gedupliceerd moeten worden door Gegevensbeheer (CPYF command); deze functie kan er eveneens voor zorg dragen, dat vertrouwelijke gegevens bij dit dupliceren worden weggefilterd.

7. Het gebruik van het Systeem/38 in de controle

Uit het voorgaande komt naar voren, dat de structuur van de S/38 uitstekende mogelijkheden biedt voor interne en externe controle. In dit hoofdstuk wordt die betekenis nader uitgewerkt voor de externe controle die zich richt op de financiële verantwoording (financial audit). Daarmee zal het tevens duidelijk zijn dat de S/38 ook van betekenis is voor de controle op de organisatie (operational audit).

Doelstelling van een financiële controle is het verkrijgen van een oordeel over een financiële verantwoording. De principiële controlemiddelen zijn het onderzoek van de organisatie waarin de gegevens zijn verzameld en verwerkt en, mede gebaseerd op conclusie uit het onderzoek van de organisatie, het onderzoek van het cijfermateriaal (pag. 52).

Onderzoek van de organisatie (compliance testing)

Indien de accountant besluit de handhaving en naleving van functiescheidingen te controleren, zal hij eerst vaststellen hoe de organisatie van de beveiliging en van het (gemeenschappelijk) gebruik van gegevens is opgezet. Hiertoe zal hij in contact treden met de Security en Gegevensbeheer functies. De CPF Command Language verschaft mogelijkheden om de beveiliging zoals die is geïmplementeerd, zichtbaar te maken. Een dergelijke controle verschaft vanzelfsprekend niet meer dan momentopnamen, waardoor het van belang is de controle zonder voorafgaande aankondiging uit te voeren. De controle is als zodanig een optimaal middel om een partieel of integraal beeld van de gehanteerde bevoegdheidsstructuur op een bepaald moment te kennen en te toetsen.

Terwille van de efficiency zal de accountant enige geautomatiseerde procedures voor het produceren van de momentopnamen moeten ontwikkelen. De controleprocedure bestaat voor een groot deel uit het zichtbaar maken van de relaties tussen gebruikers, bevoegdheden en objecten. Eveneens om redenen van efficiency zal de accountant een keuze moeten maken welke object typen, en binnen het type eventueel welke specifieke objecten, hij in zijn controle wil betrekken. Er is namelijk al gauw een groot aantal objecten in een S/38.

Stappen bij het gebruik van de computer in de controle

A. Voorbereiding

1. Kennis nemen van het beleid ten aanzien van beveiliging en het gemeenschappelijk gegevensgebruik.
2. Kennis nemen van het ontworpen systeem ten aanzien van beveiliging en het gemeenschappelijk gegevensgebruik.
3. Evalueren van beleid en systeem.
4. Voorbereiden controleprocedures.

B. Uitvoering

5. Aankoppelen onder het password van de security officer.
6. Nagaan hoe de verwerkingsomgeving eruit ziet.
7. Creëren bibliotheken, programma's, bestanden.
8. Uitvoeren CPF-commands en programma's.
9. Output en joblogs (van de batchjobs) naar de gewenste printer sturen.
10. Afkoppelen en creëren joblog interactive job.
11. Print joblog interactive job.
12. Save de bibliotheek en delete de bibliotheek.
13. Print historylog over de periode.
14. Laat security officer zijn password wijzigen.
15. Controle output en joblogs.
16. Evaluatie.

Stap 5

Sign-on onder het password van de security officer is nodig om bevoegdheid ten aanzien van alle aanwezige objecten te verkrijgen. Elk ander password verschaft een onvolledig beeld, doordat het slechts toegang verschaft tot de objecten die in het betreffende user-profile zijn vermeld (dat zijn de objecten in eigendom en de objecten waarvoor de gebruiker specifieke - private - bevoegdheden heeft gekregen) en tot de "public" objecten. Vanzelfsprekend vereist deze voorwaarde de medewerking van de security officer en instemming van de hogere leiding.

Stap 6

De accountant gaat hier na welke subsystemen hij ter beschikking heeft, welke jobdescriptions toepasbaar zijn, welke queues aanwezig zijn en naar welke printer hij het beste zijn output kan sturen.

Stappen 7/8

De accountant zal beginnen een eigen library te creëren door middel van het CRTLIB command, waarbij de public authority parameter de waarde *NONE krijgt. Vervolgens zal hij in zijn library de nodige source en data-bestanden creëren; hiervoor is het CRTPF commando (create physical file) beschikbaar: type *SRC voor de programma source-bestanden (met de standaard recordlengte 92) of type *DATA.
Sourcefiles kunnen ook zeer eenvoudig worden gecreëerd als met de Source Entry Utility wordt gewerkt (optie 8 van het programmeursmenu; het programmeursmenu kan worden bereikt door het commando CALL QPGMMENU in te toetsen op het command entry scherm; dit menu maakt het ook mogelijk op eenvoudige wijze CPF commands en programma's te laten uitvoeren, programma's naar een batch-subsysteem te sturen, in outputfiles te kijken, e.d.).

Vervolgens worden de controleprocedures ontwikkeld, waarbij gebruik wordt gemaakt van CPF commands, Command Language programma's of hogere programmeertalen (COBOL, RPG III). Indien de CPF-release CL commands bevat waarmee files kunnen worden gelezen, is het gebruik van een hogere programmeertaal niet meer nodig.

Voorbeeld

De accountant wil inzicht krijgen in de bevoegdheden ten aanzien van alle bibliotheken.
Eerst zal hij moeten weten welke bibliotheken in het systeem aanwezig zijn. Dit is mogelijk door middel van het commando "display object description":

```
DSPOBJD  OBJ(*ALL)  OBJTYPE(*LIB)
```

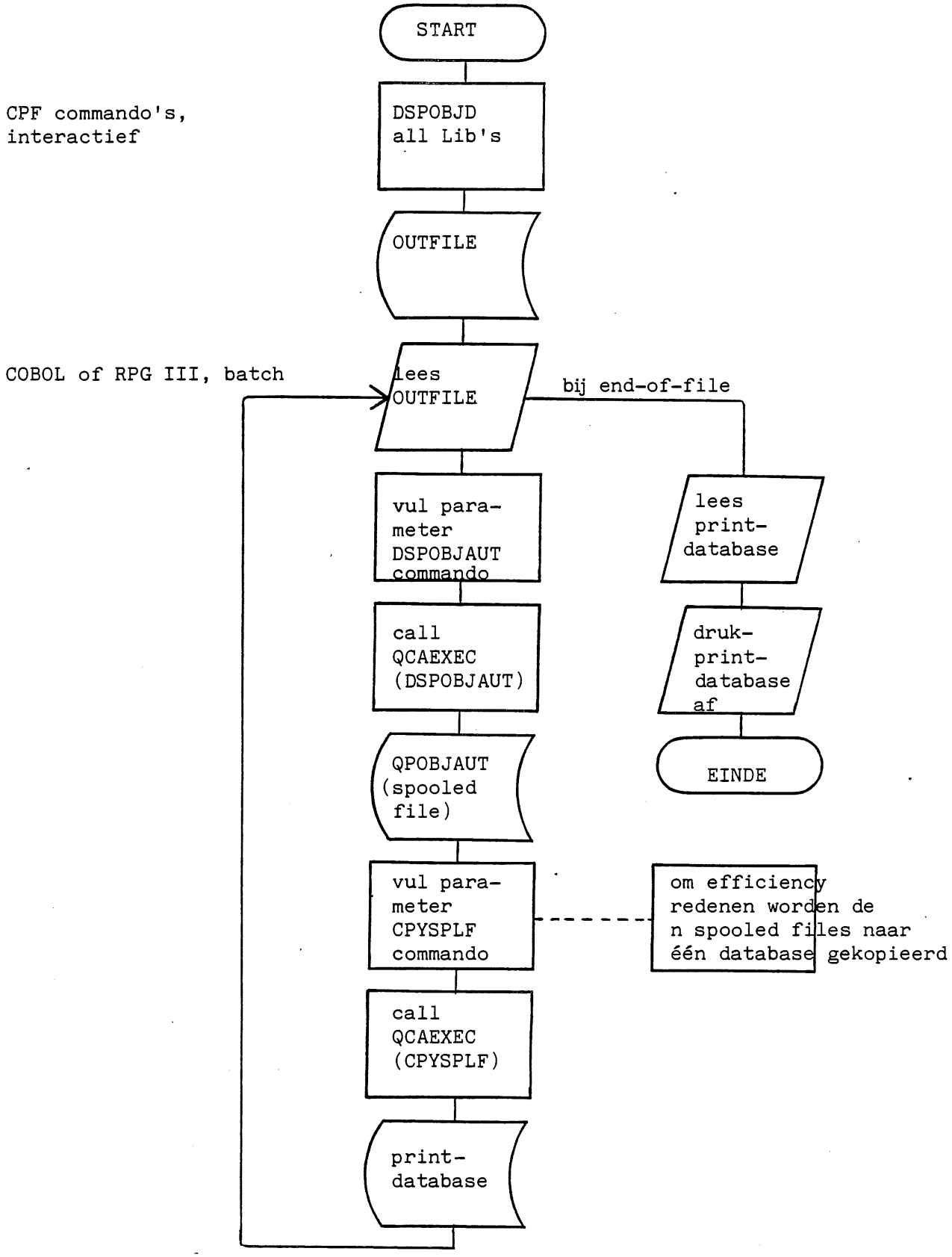
De output verschijnt naar keuze op papier of op het scherm. Daarnaast is het mogelijk de output (die de namen van alle bibliotheken bevat) in een database op te slaan, die door een COBOL, RPG III of CL-programma verder kan worden verwerkt (OUTFILE parameter).

De bevoegdheden voor libraries kunnen zichtbaar worden gemaakt door het commando "display object authority":

```
DSPOBJAUT  OBJ(library naam)  OBJTYPE(*LIB)  OUTPUT(*LIST)
```

De namen kunnen gelezen worden uit de database die met het eerste commando werd gecreëerd. Dit houdt in, dat het DSPOBJAUT commando n keer moet worden uitgevoerd, waarbij n het aantal bibliotheken is.
Om deze reden is een programma nodig dat de database leest en n keer een loop uitvoert; de loop bevat het DSPOBJAUT commando; de waarde voor de library naam in de OBJ parameter wordt op grond van de informatie in de database, steeds gewijzigd.
De loop kan vanuit een COBOL of RPG-programma worden gerealiseerd door de routine QCAEXEC aan te roepen. Deze routine stelt in staat tot het dynamisch creëren en uitvoeren van CPF commands.

Schematisch kan een en ander als volgt wordenweergegeven:



Stap 9

Na uitvoering van de geautomatiseerde procedures moet de accountant er voor zorg dragen, dat de printuitvoer naar een printer wordt gestuurd die hij onder visuele controle heeft.

Stappen 10/11

De joblog wordt gecreëerd door het SIGNOFF commando de parameter *LIST mee te geven. Joblogs zijn van belang als bewijsmateriaal terzake van wat de accountant aan commando's en programma's heeft uitgevoerd.

Stap 13

De historylog is van belang om vast te stellen dat niemand anders onder het security officer profile actief is geweest, daar in dat geval een risico van beïnvloeding heeft bestaan.

De hier vermelde controleprocedure zal als nevenvoordeel kunnen hebben, dat verwatering in de handhaving en naleving van beheersings- en beveiligingsprocedures wordt tegengegaan.

Onderzoek van het cijfermateriaal (substantive testing)

Het beoordelen en verifiëren van het cijfermateriaal kan veelal efficiënt en effectief worden ondersteund door het inschakelen van de computer in de controle. Er zijn globaal 2 mogelijkheden voor de verwerking: verwerking op de computer van de accountant en verwerking op de computer van de gecontroleerde. De eerste situatie is mogelijk door middel van fysieke bestandsoverdracht op diskette en soms ook op tape. De tweede mogelijkheid plaatst de accountant in principe in een situatie met het risico dat de gecontroleerde de verwerkingen van de accountant op ongewenste wijze beïnvloedt.

Zoals eerder is gesteld, vereisen verschillende functies in een organisatie afzonderlijke omgevingen; dit geldt eens te meer voor de onafhankelijke accountant.
De beheersings- en beveiligingsmogelijkheden zoals die werden beschreven in hoofdstuk 4, te zamen met de suggesties ten aanzien van de wijze waarop de functiescheidingen binnen de computer kunnen worden geëffectueerd in hoofdstuk 6, zullen duidelijk maken dat de accountant de S/38 van de gecontroleerde kan benutten voor het doen uitvoeren van zijn controleprogrammatuur, met voldoende garanties voor het behoud van zijn onafhankelijkheid. Hij zal echter moeten vaststellen dat de security officer niet tijdens de zelfde periode actief is geweest; dit is mogelijk door middel van de "history log" waarop alle sign-on's en sign-off's zijn vermeld.
Vanzelfsprekend moet de accountant de S/38, het CPF en de beveiligingsstructuur goed doorgronden. Een groot voordeel van de S/38 is echter, dat deze kennis op alle S/38 computersystemen toepasbaar is, omdat er slechts één CPF is; een gebruiker moet het volledig implementeren, waardoor de accountant altijd met hetzelfde operating system in aanraking komt.

Literatuur

I Linden T.A., Operating system structures to support security and reliable software, Computing Surveys Volume 8, no. 4 December 1976.

II Houden M.E. e.a., IBM System/38 support for capability based addressing, Proceedings 8th annual symposium on computer architecture 1981 (ACM, IEEE).

III A.H.C. Koedijk, De organisatie van gegevensbeheer, Compact winter 1981/1982.

IV A.W. Neisingh/A.H.C. Koedijk, Het gebruik van de computer in de Accountantscontrole, Deel I, Handboek Accountancy III, 50.

OBJECT TYPES

Objects are the basic units upon which commands perform operations. For example, programs and files are objects. Through objects you can find, maintain, and process your data on System/38. You need only know what object and what function (command) you want to use; you do not need to know the storage address of your data to use it.

There are 23 types of objects on System/38. Each type has unique purpose within the system and has associated with it a set of commands with which to process that type of object. The following lists the 23 types of objects, the abbreviations used as parameter values for object type parameters, and the definition of the object belonging to that type:

- Class (* CLS). An object that contains the execution parameters for a routing step.

- Command definition (* CMD). An object that contains the definition of a command (including the command name, parameter definitions, and validity checking information) and identifies the program that
- performs the function requested by the command.

- Control unit description (* CUD). An object that contains a description of the features of a control unit that is either directly attached to the system or attached to a communications line.

- Data area (* DTAARA). An object that contains a description of an area used to communicate data such as CL variable values between the programs within a job and between jobs.

- Device description (* DEVD). An object that contains a description of a device that is attached to the system.

- Edit description (* EDTD). An object that contains a description of a user-defined edit code.

- File (* FILE). An object that contains a description of a set of related records treated as a unit and, optionally, those records.

- Forms control table (* FCT). An object that designates the special processing requirements for specific printer or punch output streams received by an RJEF (Remote Job Entry Facility) session from a host system.

- Job description (* JOBD). An object that contains the attributes of a job.

- Job queue (* JOBQ). An object on which entries for batch jobs are placed when they are submitted to the system and from which they are selected for execution by CPF.

- Journal (* JRN). An object through which the changes made to a data base file are recorded. These changes are recorded in a journal receiver.

- Journal receiver (* JRNRCV). An object that contains entries, called journal entries, generated when a change is made to a data base file being journaled.

- Library (* LIB). An object that serves as a directory to other objects. A library is used to group related objects and to find objects by names when they are used.

- Line description (* LIND). An object that contains a description of a communications line to the system.

- Message file (* MSGF). An object that contains message descriptions.

- Message queue (* MSGQ). An object on which messages are placed when they are sent. A message queue can be associated with a person, program, work station, or job.

- Output queue (* OUTQ). An object that contains a list of output files that are to be written to an output device by a writer.

- Print image (* PRTIMG). An object that contains a description of the print belt or print train on a printer.

- Program (* PGM). An object that contains a set of instructions that tell a computer where to get input, how to process it, and where to put the results. A program is created as a result of a compilation.

- Session description (* SSND). An object that contains a description of the operating characteristics of an RJEF session.

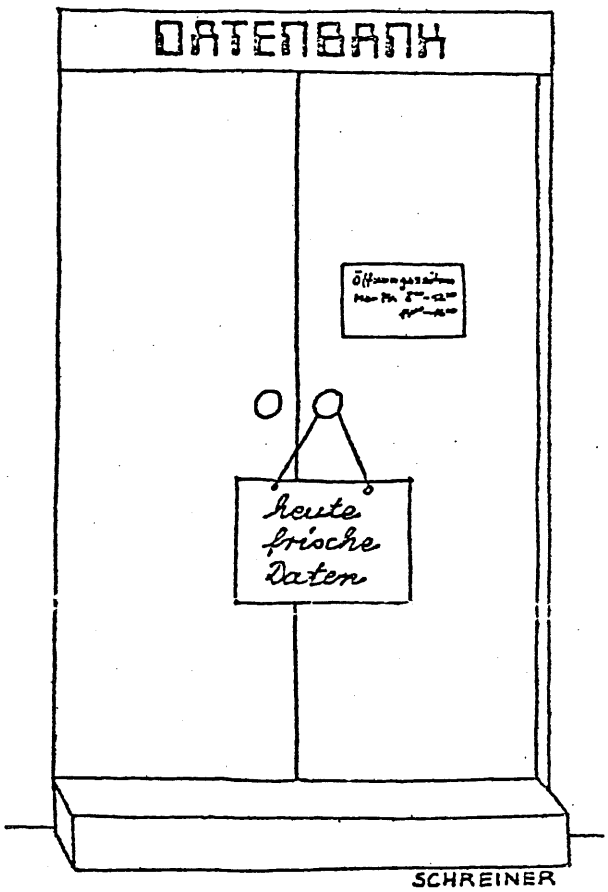
- Subsystem description (* SBSD). An object that contains the specifications that define a subsystem and that CPF uses to control the subsystem.

- Table (* TBL). An object that contains a set of hexadecimal characters used to translate one or more bytes of data.

- User profile (* USRPRF). An object that contains a description of a particular user or group of users. A user profile contains a list of the objects and functions the user is authorized to.

(Source: IBM-manual)

Das Allerletzte



CONTINUITEIT VAN DE GEGEVENSVERWERKING, EEN INLEIDING

door H. Roos

Het gebruik van slechts met een computer leesbare media voor het bewaren van informatie heeft tot gevolg dat de beschikbaarheid van de informatie mede afhankelijk is van de goede werking van de computer en van de kwaliteit van de gebruikte opslagmedia.

Het artikel van R. Bron (zie pag. 8) over back-up, restart en recovery heeft betrekking op de maatregelen die kunnen worden getroffen om te voorkomen dat informatie, die op dergelijke media wordt bewaard, verloren gaat.

De aard van de te treffen maatregelen is afhankelijk van de eigenschappen van het toegepaste medium wat betreft het vasthouden van de informatie onder verschillende omstandigheden, de snelheid waarmee een willekeurige eenheid informatie op het medium kan worden aangebracht en kan worden teruggevonden, alsmede de opslagcapaciteit van het medium.

In de meeste gevallen zal de in het interne geheugen opgeslagen informatie slechts beschikbaar blijven zolang de stroomtoevoer naar de computer niet wordt onderbroken. Dit euvel kan gedeeltelijk worden ondervangen door de computerinstallatie te voorzien van een batterij die er voor kan zorgen dat, na een onderbreking van de normale stroomtoevoer via het openbare net, de computer nog enige tijd onder spanning blijft om de gelegenheid te bieden de informatie uit het interne geheugen naar een extern medium over te brengen.
Magneetbanden, magneetschijven en floppies zijn voor het behoud van de erop vastgelegde informatie niet van de handhaving van de stroomtoevoer afhankelijk en bieden daardoor een scala van mogelijkheden voor het over langere tijdsperioden vasthouden van informatie. De op die media vastgelegde informatie kan echter uitsluitend worden zichtbaar gemaakt door middel van een computerproces. Een belangrijke eigenschap van magneetbanden, floppies en magneetschijven van het verwisselbare type is de mogelijkheid om de erop vastgelegde informatie zichtbaar te maken via een andere computer dan waarmee die informatie is vastgelegd. De informatie op niet verwisselbare schijven is alleen via de computer waarmee die is vastgelegd ook weer zichtbaar te maken.
De tijdsduur waarover deze media de informatie onverminkt kunnen conserveren hangt af van onder meer de fysieke kwaliteit. De vaste schijven bieden bij de huidige stand der techniek een aanmerkelijk hogere kwaliteit dan de verwisselbare media. Voorts heeft de groei van toepassingen die de informatie zeer snel na opvragen beschikbaar maken ertoe geleid dat zowel de opslagcapaciteit van schijven als de snelheid waarmee de overdracht van informatie tussen het interne geheugen en de schijf plaatsvindt, aanzienlijk zijn toegenomen. Deze technische verbeteringen hebben evenwel in hoofdzaak betrekking op vaste schijven, omdat banden en verwisselbare schijven hiervoor te kwetsbaar zijn gebleken.

Bij de huidige stand der techniek bestaan er grote verschillen in opslagcapaciteit tussen de verschillende media en tussen de daarbij behorende overdrachtssnelheden.
Intern geheugen is zeer snel doch, ondanks de vrijwel continu dalende prijzen per eenheid opgeslagen informatie naar verhouding van beperkte capaciteit.
Vaste schijven bieden zeer grote opslagcapaciteit, tot ca. 1.000 gigabyte per schijf die niet sequentieel (random) kunnen worden gelezen en geschreven met overdrachtssnelheden in de orde van 3.000 kilo-bytes per seconde (kbps).
Banden zijn in verschillende lengtes beschikbaar. De opslagcapaciteit is sterk afhankelijk van de dichtheid waarmee de informatie wordt opgeslagen - van ca. 550 bytes per inch (bpi) tot 6.250 bpi - en van de overdrachtssnelheid, van 470 kbps tot 1.250 kbps.
Het is uiteraard wenselijk om uit dit brede scala van mogelijkheden een voor elke situatie zo optimaal mogelijke te kiezen. Bij het maken van afwegingen kunnen verschillende toepassingen op eenzelfde installatie een onderling strijdige oplossing vereisen.

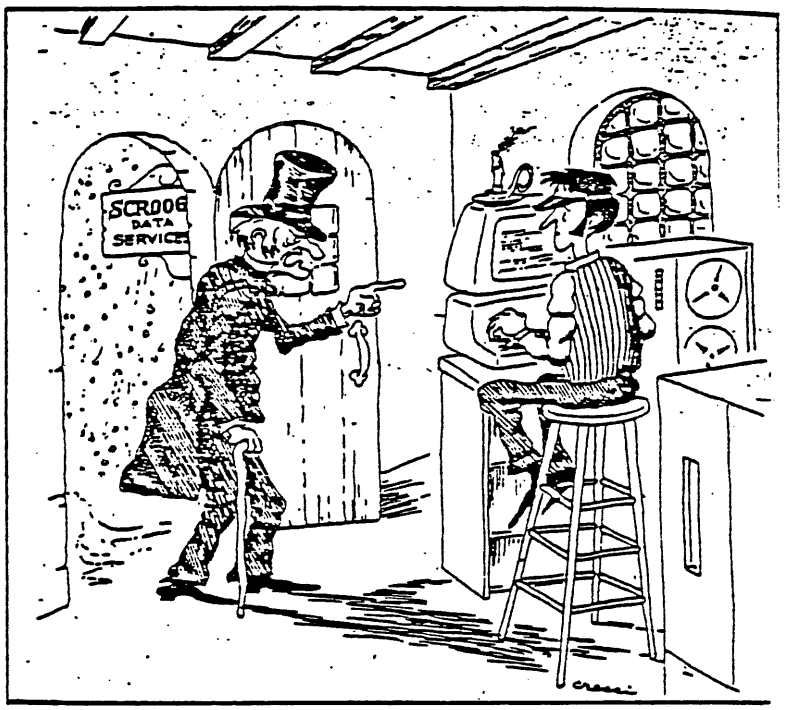
Essentieel is dat zowel tijdens een opslagoperatie, als tijdens een terugzoekoperatie, de informatie altijd tijdelijk is opgeslagen in het interne geheugen van de computer waarmee die operaties worden bestuurd. Dit betekent dat nieuwe informatie verloren kan gaan voordat die op een extern medium is opgeslagen.

Een tweede factor is de maximale tijdsduur die mag verstrijken tussen het moment waarop een bepaalde eenheid informatie wordt opgevraagd en het tijdstip van beschikbaar komen. Naarmate het bedrijfsproces waarvoor de gevraagde informatie bestemd is voor een goed functioneren sterker afhankelijk is van het snel over die informatie kunnen beschikken zullen er hogere eisen worden gesteld aan de snelheid waarmee verloren gegane informatie moet kunnen worden gereconstrueerd.

In essentie komen alle mogelijke maatregelen erop neer dat de informatie, die moet worden beschermd tegen verlies, op meer dan een medium wordt opgeslagen.
Dit roept het probleem op van de gelijkloop van de verschillende opgeslagen versies van de informatie.
De wijze waarop dit kan worden geregeld hangt tevens samen met de maatregelen die worden getroffen om te kunnen vaststellen dat opgeslagen informatie volledig en juist is en blijft. Deze integriteitscontroleprocedures moeten worden gesynchroniseerd met de back-up, recovery en restart procedures.
De vorm van deze procedures wordt voorts sterk beïnvloed door de organisatie van de processen voor het opslaan en opvragen van informatie.

Een proces waarbij slechts één aan een bepaalde bedrijfseenheid gebonden opvraag- en opslagcyclus tegelijk mogelijk is, kan met eenvoudiger procedures worden beveiligd, dan een proces dat tegelijkertijd meer dan een opslag- en opvraagcyclus toestaat. In het tweede geval zijn maatregelen nodig ter voorkoming van informatieverlies doordat vanuit twee verschillende bronnen dezelfde informatie-eenheid kan worden gewijzigd.

Hiervoor wordt normaliter gebruik gemaakt van de "concurrency-control" procedures van de speciale database management software. Dergelijke standaardprocedures gaan echter uit van bepaalde veronderstellingen die niet steeds stroken met de wijze van programmeren van toepassingen.
De zogenaamde "recoverable transactie" volgens de standaard concurrency control procedure dekt niet steeds de transactie die in het kader van een bepaalde toepassing "recoverable" moet zijn.
Een transactie is "recoverable" zolang het effect ervan op de opgeslagen en verstrekte informatie kan worden teniet gedaan.
Hieraan kan worden voldaan indien en voor zover per transactie een vastlegging wordt gemaakt van alle informatie die is uitgewisseld tussen de persoon of het proces dat de transactie gebruikt en de opgeslagen informatie.
Voor transactiesoorten die gelijktijdig meer dan één transactie toestaan, houdt dit onder meer in dat de transactievolgorde een rol speelt.



'Christmas . . . Bah! You're Not Leaving Until You Finish Tha General Ledger Program.'

In het in dit nummer en het volgende op te nemen opstel van de hand van R. Bron, wordt in extenso ingegaan op fundamentele technieken voor het voorkomen van verlies van op externe media opgeslagen informatie.

Op de implicaties van concurrency-control en van de recovery van transacties zal in een afzonderlijk opstel worden ingegaan.

Back-up, restart en recovery door R. Bron is als volgt ingedeeld:
In deze aflevering van Compact
1. Inleiding.
2. Back-up, recovery en restart: een historisch perspectief.
3. Back-up.
3.1 Techniek van back-up per categorie.
    A. Besturingssysteem en overige harde software (utilities).
    B.1 Toepassingsprogrammatuur (source-coding).
    B.2 Toepassingsprogrammatuur (object-coding).
    C. Job Control Language (de karweibesturingstaal).
    D. Gegevensbestanden:
        - batch-verwerking (generatieprincipe);
        - data entry;
        - real time on-line.
    E. Object versus medium.
3.2 Mengvorm object en medium gerichte techniek.
In het herfstnummer 1983 van Compact komen vervolgens aan de orde:
4. Recovery en restart.
4.1 Voorbeeld situatie.
4.2 Gebruik van log-bestanden.
    A. Before en after images.
    B. Alleen before images.
    C. Alleen after images.
    D. De mutaties zelf.
5. Specifieke aspecten.
    A. Besturingssysteem en overige harde software (utilities)
    B. Gegevensbestanden.
6. Controle-implicaties.
6.1 Procedures en voorschriften.
    A. Besturingssysteem en overige harde software.
    B. Toepassingsprogrammatuur (source-coding).
    C. Job Control Language.
    D. Gegevensbestanden.
6.2 Registratie van bestanden.
6.3 Bruikbaarheid van back-up kopieën.
7. Tenslotte.

COMPACT

Zomer 1983

BACK-UP, RESTART EN RECOVERY

door R. Bron

1. Inleiding

Bij de geautomatiseerde gegevensverwerking is het - naast de betrouwbaarheid van de systemen - van belang dat de continuïteit gewaarborgd wordt.
Om het bestaan van procedures en voorschriften gericht op de continuïteit vast te stellen, worden in voor de controle gebruikte hulpmiddelen (checklisten) veelal summiere vragen aangetroffen op het gebied van "beveiliging van informatiedragers". Daarmee wordt dan dit gebied als afgedekt beschouwd.
Bovendien worden bij het aspect "continuïteit" direct de begrippen Back-up en Restart of Restart en Recovery in één adem genoemd zonder dat stilgestaan wordt bij de problematiek, welke daarachter schuilgaat.

Doel van het artikel is de lezer inzicht te geven in die complexiteit en hem/haar de helpende hand te bieden bij het onderkennen van de problemen in verschillende praktijksituaties.
Om het artikel in enigerlei mate beperkt te houden wordt slechts ingegaan op hetgeen zich binnen een rekencentrum afspeelt.
In hoofdstuk 2 wordt een overzicht gegeven van de ontwikkeling van Back-up, Recovery en Restart gezien vanuit een historisch perspectief.
Daarna wordt in de hoofdstukken 3 en 4 ingegaan op mogelijke Back-up, Recovery en Restart-technieken.
Behandeling van specifieke aspecten vindt plaats in hoofdstuk 5; op de controle-implicaties wordt nader ingegaan in hoofdstuk 6.

2. Back-up, Recovery en Restart: een historisch perspectief

In de prehistorie van de automatisering werd de continuïteit van de gegevensverwerking gewaarborgd door organisatorische maatregelen met betrekking tot de opslag en bewaring van de bij de verwerking gebruikte ponskaarten. Een van de problemen hierbij was het volledig blijven van de kaartenbestanden. Daarnaast werd meestal vanwege de kwantitatieve verhoudingen geen kopieën van bestanden aangemaakt en elders bewaard. Bij de opkomst van magnetiseerbare media (welke voornamelijk betekenis heeft gehad op de verwerkingssnelheid) kwam eigenlijk het aspect Back-up, Recovery en Restart om de hoek kijken. Periodiek werden kopieën van gegevensbestanden gemaakt waarop in geval van meer of minder langdurige storing kon worden teruggevallen.

De continuïteit van de gegevensverwerking werd in belangrijke mate bepaald door de aanwezigheid van kopieën van mutatiebestanden. De omgeving waarin de verwerking plaatsvond (single programming, multiprogramming en/of multiprocessing) was hierop niet van invloed.

Onder single programming wordt verstaan die verwerkingsomgeving waarbij één programma de beschikking heeft over de gehele computer. Bij multiprogramming is het interne geheugen van de computer verdeeld in parten (van gelijke of ongelijke grootte), partities genaamd. Elke partitie kan één programma bevatten. Het daadwerkelijk actief zijn van het programma is afhankelijk van het aantal processoren. Een processor kan op enig moment slechts 1 proces (de uitvoering van een programma) behandelen. Bij multiprogramming is slechts 1 processor beschikbaar.
Van multiprocessing is sprake als meerdere processoren aanwezig zijn voor de gegevensverwerking.
Vanwege de steeds complexer wordende automatisering is het thans niet meer terecht Back-up, Recovery en Restart in één adem te noemen. Zowel Back-up als Recovery en Restart zijn een eigen leven gaan leiden in die zin dat voor het uitvoeren van Back-up, Recovery en Restart niet altijd kopieën van bestanden nodig zijn.
Nieuwe Recovery en Restart-technieken hebben hun intrede gedaan.
Back-up dient te worden geassocieerd met continuïteit op lange termijn; Recovery en Restart is korte termijn gericht.

3. Back-up

In hoofdstuk 2 is aangegeven dat back-up gericht is op het waarborgen van de continuïteit op langere termijn.
Dit wordt gerealiseerd door het kopiëren van bestanden met een bepaalde frequentie (generatiesysteem).
Hierbij komt de vraag op van welke bestanden kopieën nodig zijn om de continuïteit op langere termijn redelijk te kunnen waarborgen. In eerste instantie wordt daarbij meestal gedacht aan gegevensbestanden. Bij nader inzien is de continuïteit slechts te waarborgen als van de volgende categorieën de juiste kopiebestanden beschikbaar zijn:

a. het besturingssysteem en overige harde software;
b. toepassingsprogrammatuur;
c. job control language;
d. gegevensbestanden.

De registraties van bestanden zijn niet onder deze categorieën opgenomen, doch worden behandeld in hoofdstuk 6 "Controle-implicaties" paragraaf 3.

De manier waarop kopieën worden gemaakt kan vanuit twee invalshoeken worden benaderd:

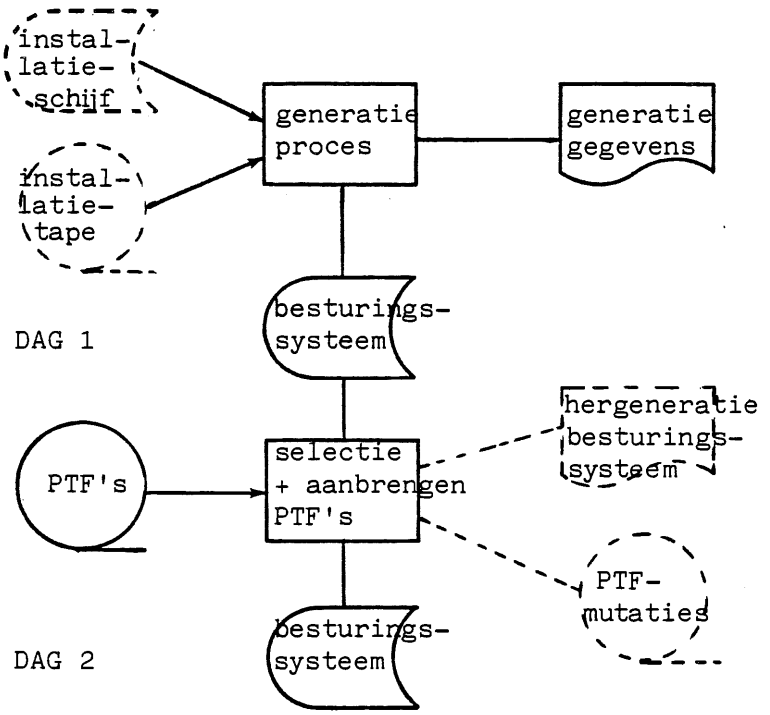
- object gericht;
- medium gericht
- combinatie.

Het frequentie-aspect dat onder andere wordt bepaald door de factoren financiële middelen, alternatieve mogelijkheden om verloren gegane delen te herstellen, blijft verder buiten beschouwing.

3.1 Techniek van back-up per categorie

A. Besturingssysteem en overige harde software (utilities)

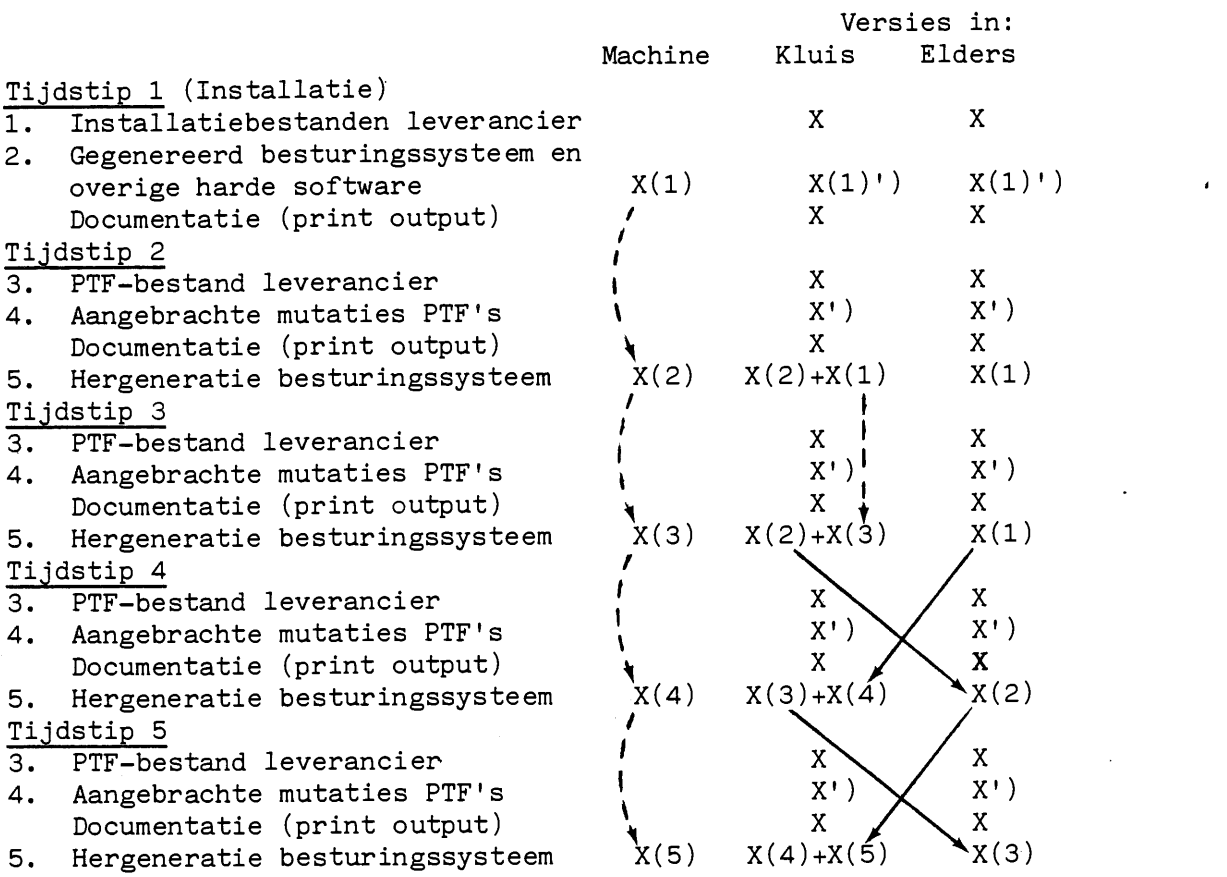
Generatie van het besturingssysteem heeft veelal plaatsgevonden op basis van de van de leverancier ontvangen installatietapes of schijf.
Wijzigingen op het besturingssysteem aangebracht door de leverancier (Program Temporary Fixes (PTF's)) worden veelal op magneetband aangeleverd.
Daarnaast kunnen eigen wijzigingen worden aangebracht.
Het voorgaande is schematisch weergegeven in figuur 1.



Figuur 1.

In figuur 2 wordt een uitwerking gegeven.
Hierin wordt de volgtijdelijke beweging aangegeven van de bestanden tussen de kluis en bewaring elders.
Een "X" in de kolommen geeft de fysieke plaats, waar de (kopie)bestanden worden aangetroffen, aan.
Tussen haakjes ( ) wordt het versienummer gegeven.
De ononderbroken lijnen geven de verplaatsing weer tussen de locaties en (mogelijk) hergebruik van het medium.
Uitgegaan wordt van de aanwezigheid van meerdere generaties (3) aangevuld met de basisgeneratie en alle in de loop van de tijd hierop aangebrachte wijzigingen (PTF (Program Temporary Fixes)-mutaties).

Ideale beveiligingssituatie besturingssysteem en overige harde software



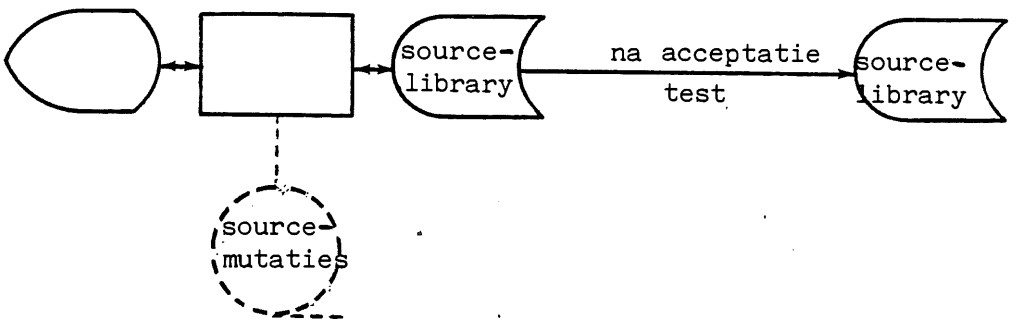
Figuur 2.

') De basisgeneratie X(1) en alle hierop in de loop van de tijd aangebrachte wijzigingen (PTF-mutaties) dienen aanwezig te zijn naast de aangegeven (her)generaties.

B.1 Toepassingsprogrammatuur (source-coding)

Bij toepassingsprogrammatuur wordt niet direct aan gegevensverzamelingen (bestanden) gedacht.
Echter ten onrechte. Het is een gegevensverzameling. Programmatuur wordt opgeslagen op magneetband, schijf, etc. en ondergebracht in bibliotheken. Hierbij kan tevens onderscheid worden gemaakt in enerzijds opslag source-coding ten behoeve van systeemontwikkeling/onderhoud en anderzijds source-coding ten behoeve van produktie.
Uit betrouwbaarheidsoogpunt dienen deze bibliotheken gescheiden te zijn (zie figuur 3).

Systeemontwikkeling/onderhoud | Produktie



Figuur 3.

Voor systeemontwikkeling en onderhoud gelden twee afzonderlijke technieken.
In de praktijk wordt in de produktiesfeer meestal volstaan met het maken van twee kopieën van de gehele source-library, elke keer dat er zich iets wijzigt met gescheiden opslag van de kopieën (object gericht). Hierbij wordt geen generatiesysteem bijgehouden.
In de ontwikkelingssfeer waar mutaties real time on-line worden aangebracht, vindt kopiëren van bestanden meestal met een grote interval plaats. Dit vanwege het feit dat het geen direct verband houdt met de continuïteit van de gegevensverwerking in de produktiesfeer.
Er mag niet aan worden voorbijgegaan dat verlies van data met hoge kosten gepaard kan gaan.

In figuur 4 wordt de beweging van de back-up bestanden bij een 3-generatiesysteem (object gericht) weergegeven.

Back-up schema source-library systeemontwikkeling/onderhoud

	Machine	Kluis	Elders
Periode 1			
- Source-library	X(1)	X(1)	X(1)
- Mutaties		M(1)	M(1)
Periode 2			
- Source-library	X(2)	X(2)+X(1)	X(1)
- Mutaties		M(2)+M(1)	M(1)
Periode 3			
- Source-library	X(3)	X(3)+X(2)	X(1)
- Mutaties		M(3)+M(2)	M(1)
Periode 4			
- Source-library	X(4)	X(4)+X(3)	X(2)
- Mutaties		M(4)+M(3)	M(2)

Figuur 4.

B.2 Toepassingsprogrammatuur (object-coding)

Voor de object-coding zijn geen specifieke beveiligingsmaatregelen vereist immers bij een adequate beveiliging van de source-coding is de object-coding altijd door hercompilatie opnieuw te verkrijgen. De computertijd benodigd voor hercompilatie bepaalt in belangrijke mate het kostenniveau.
Om die reden wordt ook wel een éénmalige kopie getrokken, direct na compilatie.

C. Job Control Language (de karweibesturingstaal)

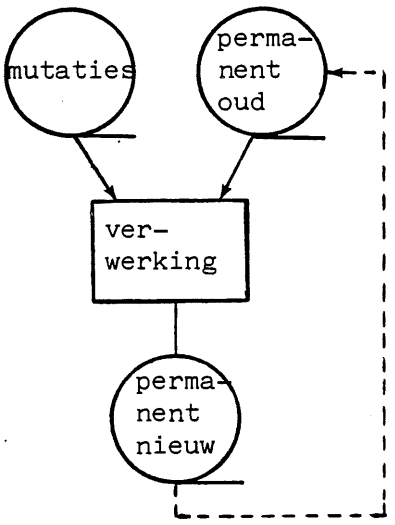
De registratie van de Job Control Language (JCL) geschiedt op magneetschijf, op ponskaart of een mengvorm van beide.
Met dit laatste wordt bedoeld dat met één (of enkele) ponskaart(en) de gehele job-definitie (de JCL-stream) wordt opgeroepen en voor uitvoering in de jobqueue (Readerqueue) wordt gezet. Een queue is een wachtkamer (vergelijkbaar met die van een tandarts).
Een mechanisme binnen de computerinstallatie selecteert hieruit de uit te voeren programma's.
Voor zover de JCL op magneetschijf staat kan deze real time on-line worden aangepast (bijvoorbeeld ten aanzien van wijziging van benodigde bestanden, e.d.).
Voor de continuïteit van de gegevensverwerking is slechts de JCL in de produktiesfeer van belang.
De back-up techniek is identiek aan het beschrevene onder "Toepassingsprogrammatuur" (source-coding) met betrekking tot systeemontwikkeling/onderhoud.
De JCL-ponskaartvorm wordt handmatig gewijzigd waardoor eveneens een nieuwe versie ontstaat.
Back-up kopieën zijn niet aanwezig. Voor het continuïteitsaspect is het van belang dat de gehele JCL-stream goed gedocumenteerd is om reconstructie mogelijk te maken. Hierbij dienen beveiligingseisen aan de documentatie te worden gesteld.

D. Gegevensbestanden

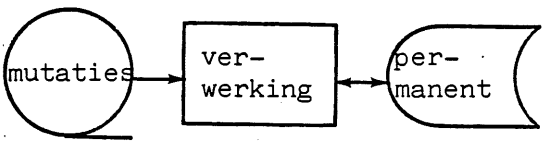
Dit zijn van oudsher de bestanden die uit continuïteitsoverwegingen de meeste aandacht hebben en hebben gekregen. De meest bekende techniek is het maken van kopieën volgens het generatieprincipe. In het magneetbandtijdperk was het maken van een kopie zowel medium- als objectgericht. Bij de introduktie van de schijf vond een verschuiving plaats naar objectgericht.
Uit efficiency-overwegingen werd later gekozen voor de mediumgerichte techniek. Hierop wordt nader ingegaan in paragraaf 3.2.
De gekozen techniek wordt mede bepaald door de verwerkingsomgeving. Ingegaan wordt op batch-verwerking (figuur 5), uitgestelde batch-verwerking (Data entry) figuur 7 en real time on-line-verwerking (figuur 8).

BATCH-VERWERKING (generatieprincipe)

a



b



Figuur 5.

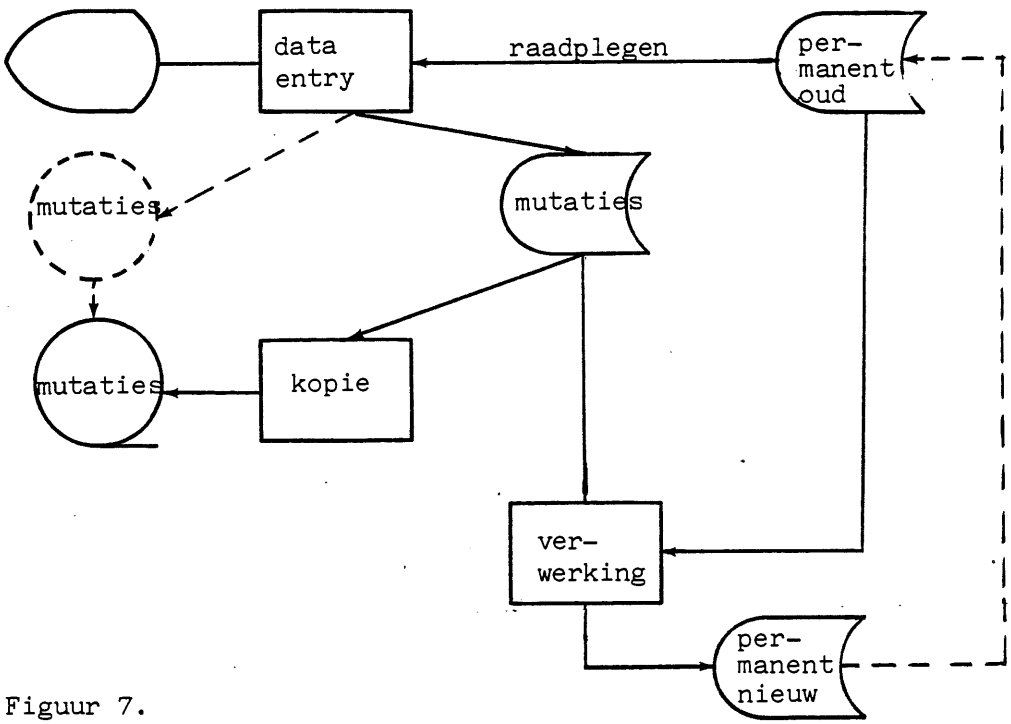
In de situatie sub a, waarbij alle bestanden op magneetband aanwezig zijn, wordt volstaan met het bewaren van permanente bestanden volgens een generatiesysteem (minimaal 3 generaties) aangevuld met mutatiebestanden (minimaal 2 generaties) (zie figuur 6).

	Machine	Kluis	Elders
Periode 1	P(0)	P(0)	
- Mutaties		M(1)	M(1)
- Permanent bestand	P(1)	P(0)+P(1)	P(0)
Periode 2			
- Mutaties		M(2)	M(1)
- Permanent bestand	P(2)	P(1)+P(2)	P(0)
Periode 3			
- Mutaties		M(3)	M(2)
- Permanent bestand	P(3)	P(2)+P(3)	P(1)
Periode 4			
- Mutaties		M(4)	M(3)
- Permanent bestand	P(4)	P(3)+P(4)	P(2)

Figuur 6.

Voor de situatie sub b, wordt verwezen naar het back-up schema source-library systeemontwikkeling/onderhoud (figuur 4).

DATA ENTRY



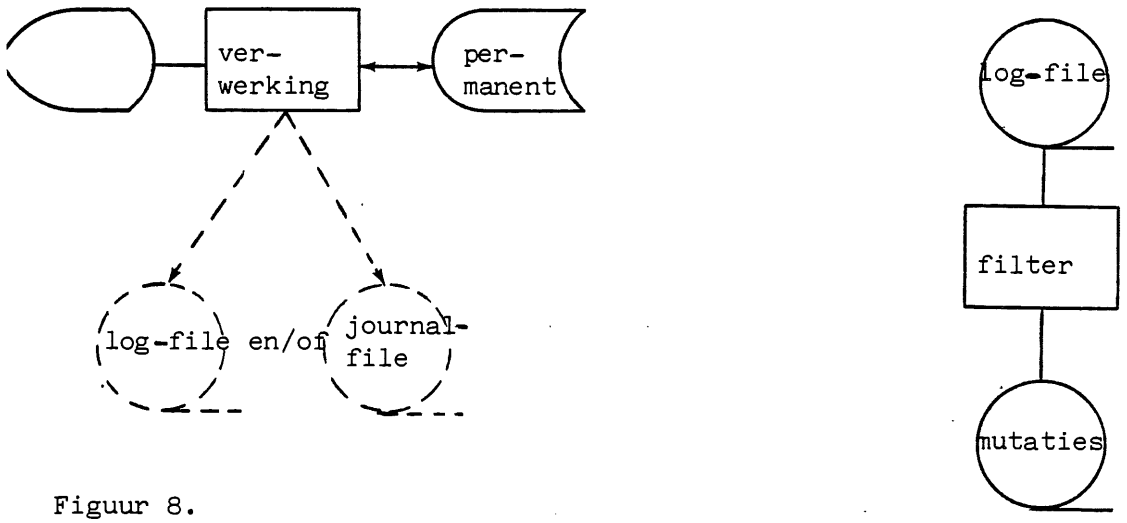
Figuur 7.

Data entry (ook wel uitgestelde batch-verwerking genoemd) kan voor wat betreft de beveiligingsproblematiek beschouwd worden als identiek aan het beschrevene onder de batch-verwerking.

De mutaties worden in de periode tussen twee verwerkingen weggeschreven naar:
- magneetschijf of magneetband;
- magneetschijf en ook naar magneetband;
- andere magnetiseerbare externe geheugenvormen.

Voor zover de mutaties alleen op magneetschijf worden weggeschreven, is het aan te bevelen een kopie te maken van het mutatiebestand op magneetband alvorens de verwerking wordt gestart.
Hierdoor wordt voorkomen dat bij het zich voordoen van een calamiteit de mutaties verloren gaan en derhalve opnieuw moeten worden ingevoerd.

REAL TIME ON-LINE



Figuur 8.

Bij real time on-line systemen worden mutaties direct op het bestand aangebracht.
Registratie van mutaties is noodzakelijk om het geheel controleerbaar te houden.
Standaard software die real time on-line-verwerking mogelijk maken, bieden de mogelijkheid of dwingen af om mutaties op een apart medium vast te leggen. Dit medium is een log en/of journalfile.
Hierbij kunnen zich 3 situaties voordoen:
1. journalfile;
2. logfile;
3. gecombineerde log/journalfile.

Ad 1.

De journalfile kan de volgende informatie bevatten:
- before images: dat wil zeggen de stand van het gemuteerde record voordat de wijziging geëffectueerd wordt;
- after images: dat wil zeggen de stand van het gemuteerde record na effectuering van de wijziging;
- before en after images;
- de mutaties zelf.

Ad 2.

Worden de mutaties geregistreerd op een logfile, dan zijn zij vermengd met andere systeemboodschappen (zoals logon/logoff, foutboodschappen, e.d.) en dient speciale programmatuur gebruikt te worden om deze mutaties "eruit" te filteren.

Ad 3.

Wordt naast de logfile gebruik gemaakt van een journalfile dan bevat de logfile alleen systeemboodschappen.
De informatie op de journalfile is reeds weergegeven in ad 1.
De journalfile en de "gefilterde" log file zijn te beschouwen als mutatiebestanden.
Om deze reden kan voor de back-up techniek worden verwezen naar het back-up schema source-library systeemontwikkeling/onderhoud (figuur 4).

E. Object versus medium

In hoofdstuk 3 zijn de vier categorieën aangegeven waarop back-up technieken zich dienen te richten, namelijk:
- het besturingssysteem;
- toepassingsprogrammatuur;
- job control language;
- gegevensbestanden.

Bovendien is genoemd dat kriteria kunnen leiden tot object c.q. medium gerichte wijze van het kopiëren van bestanden.
Onder object gericht wordt verstaan dat van een specifiek bestand') - van welke categorie dan ook - een kopie wordt gemaakt.
Van medium gericht kopiëren wordt gesproken als het maken van kopieën niet gericht is op een bestand maar op de informatiedrager waarop het bestand staat.

In de hierna volgende tabel (figuur 9) is aangegeven op welke media de diverse categorieën kunnen worden aangetroffen. De keuze van de back-up techniek (object c.q. medium gericht) wordt bepaald door:
- de door gebruikers gestelde (extra) eisen (bijvoorbeeld kritische gegevensverzamelingen);
- technische en efficiency gerichte overwegingen.

In de praktijk zal het voorkomen dat één of meerdere objecten op één of meerdere informatiedragers zijn geplaatst.

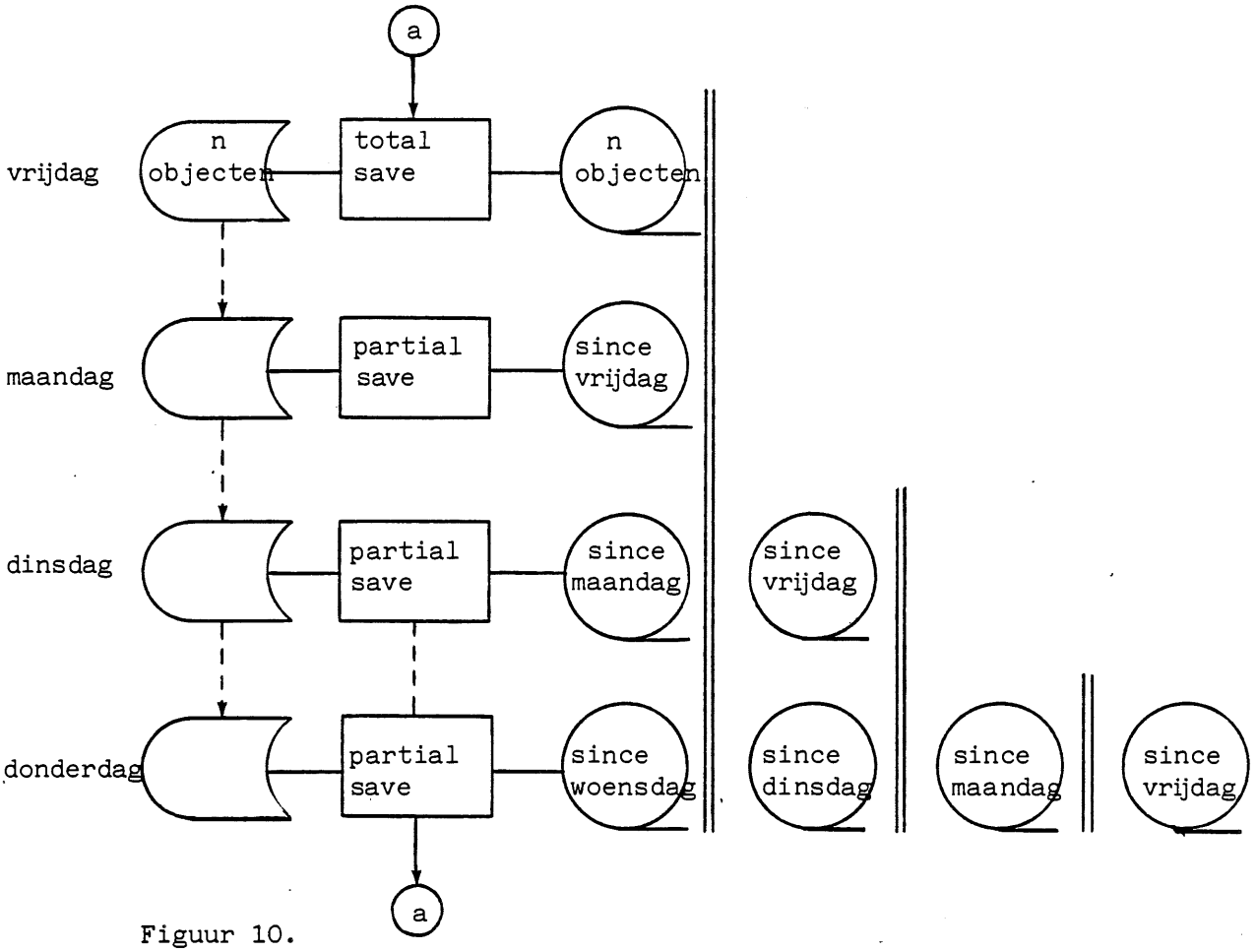
') In de zin van een "logisch" bestand. Dit bestand kan op grond van meerdere redenen (bijvoorbeeld omvang) over meerdere fysieke informatiedragers verdeeld zijn.

Object \ Medium	Magneetschijf	Magneetband en overige magnetiseerbare media	Ponskaart
A. Besturingssysteem en overige harde software	X	X	
(utilities)	X	X	
B. Toepassingsprogrammatuur			
B.1 Source-coding	X	X	X
B.2 Object-coding	X	X	
C. Job Control Language	X		X
D. Gegevensbestanden	X	X	X

Figuur 9.

3.2 Mengvorm object en medium gerichte techniek

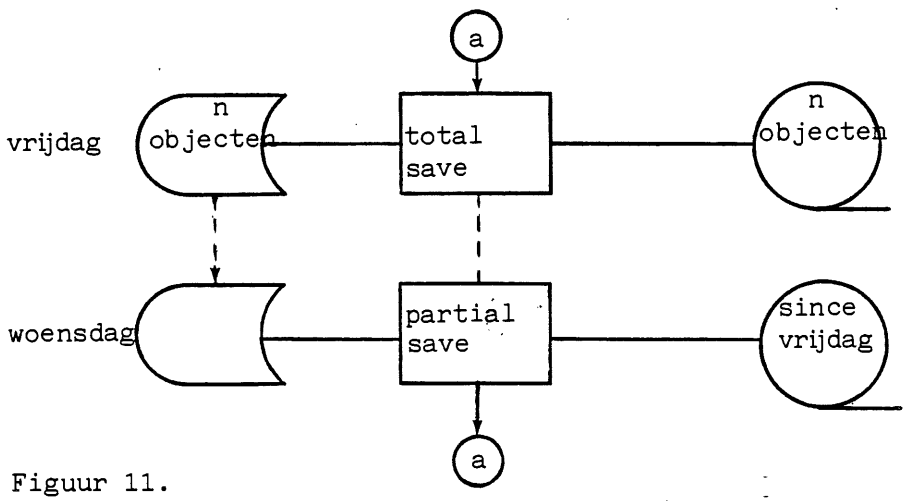
Naast de object en medium gerichte techniek komt een mengvorm voor. Deze bevat aspecten van beide technieken.
Uitgangspunt hierbij is het medium. Dit wordt meestal bepaald door technische aspecten. Bij vaste schijven is het uit beveiligingsoogpunt noodzakelijk dat een kopie van de daarop vermelde informatie elders aanwezig is. Meestal wordt gestart met het dagelijks kopiëren van de vaste schijf. Na verloop van tijd blijkt dat slechts bepaalde bestanden (objecten) frequent worden gemuteerd. Het blijkt dat het dan doelmatiger is dagelijks de gemuteerde objecten te kopiëren. Gekopieerd worden het object en de datum van laatste wijziging. Dit laatste wordt uit de index van de informatiedrager gehaald.
Periodiek wordt de totale informatiedrager gekopieerd.
Hoewel deze mengvorm voornamelijk bij vaste schijven wordt gehanteerd komt zij ook bij verwisselbare schijven voor.



Figuur 10.

In figuur 10 is één en ander schematisch weergegeven.

Het is zeer wel mogelijk het tijdsinterval tussen het maken van back-up kopieën te vergroten. Het risico van verlies in geval van calamiteit wordt daardoor echter vergroot.
Het schema (figuur 11) wordt dan als volgt:

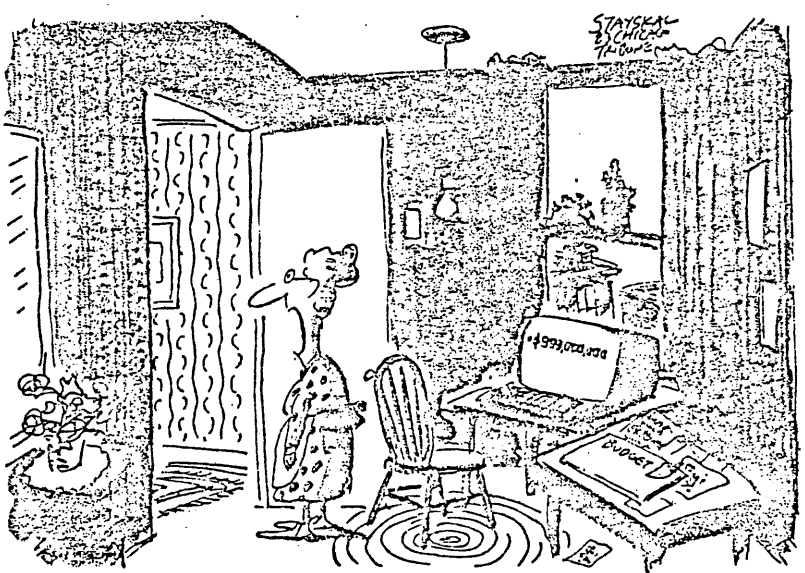


Figuur 11.

In voorgaande paragrafen is gesproken over object c.q. medium gerichte technieken alsmede een mengvorm.
De complexiteit van de gehele materie wordt vergroot door het feit dat deze technieken naast elkaar kunnen voorkomen binnen één en dezelfde produktie omgeven. De waarschuwing is op zijn plaats in de praktijk niet uit te gaan van "een back-up procedure". Het is verstandiger na te gaan of er meerdere zijn. Een antwoord als "Als back-up systeem wordt het generatieprincipe gehanteerd" is op zich niet veelzeggend.
Dit systeem kan binnen elke - in voorgaande - gehanteerde techniek voorkomen. Het gaat erom wat wordt gekopieerd en welk risico van gegevensverlies bestaat in geval van calamiteit. Hierbij dient niet uit het oog te worden verloren dat van alle categorieën de vereiste back-up kopieën zijn gemaakt om ingeval van calamiteit de continuïteit van de gegevensverwerking in redelijke mate te kunnen waarborgen.


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

. . . und Bild



"HENRY, DID YOU DEPOSIT 993 MILLION DOLLARS TODAY, OR DID I GET INTO THE 1ST NATIONAL BANK'S COMPUTER AGAIN?"

BACK-UP, RESTART EN RECOVERY

(deel 2)

door R. Bron

4. Recovery en Restart

In het eerste deel van dit artikel is gesteld dat het niet meer terecht is Back-up, Recovery en Restart in één adem te noemen.
Voor het uitvoeren van een succesvolle Recovery en Restart zijn niet in alle gevallen back-up kopieën noodzakelijk. Dit is mede afhankelijk van de soort storing/calamiteit (variërend van deelbeschadiging van een object tot algehele vernietiging van de informatiedrager).
Deze uitspraak verdient nadere nuancering.
Voor de categorieën besturingssysteem, toepassingsprogrammatuur en job control language zal in alle gevallen teruggegrepen moeten worden op de laatst aanwezige kopie.
De recovery techniek dient parallel te lopen met de back-up techniek (object of medium gericht).

Bij de categorieën gegevensverzameling is de situatie zodanig gewijzigd dat bij de Recovery en Restart gebruik wordt gemaakt van technieken waarmee niet terug hoeft te worden gevallen op back-up kopieën. Dit is het geval wanneer sprake is van real time on-line-verwerking.

Alvorens op de aspecten bij real time on-line-verwerking wordt ingegaan, volgt eerst een uiteenzetting over een speciale recovery techniek die in de praktijk voorkomt en betrekking heeft op alle vier categorieën (de mengvorm object en medium gericht).
Hierbij is een tweetal varianten mogelijk (zie figuur 12).

Variant a

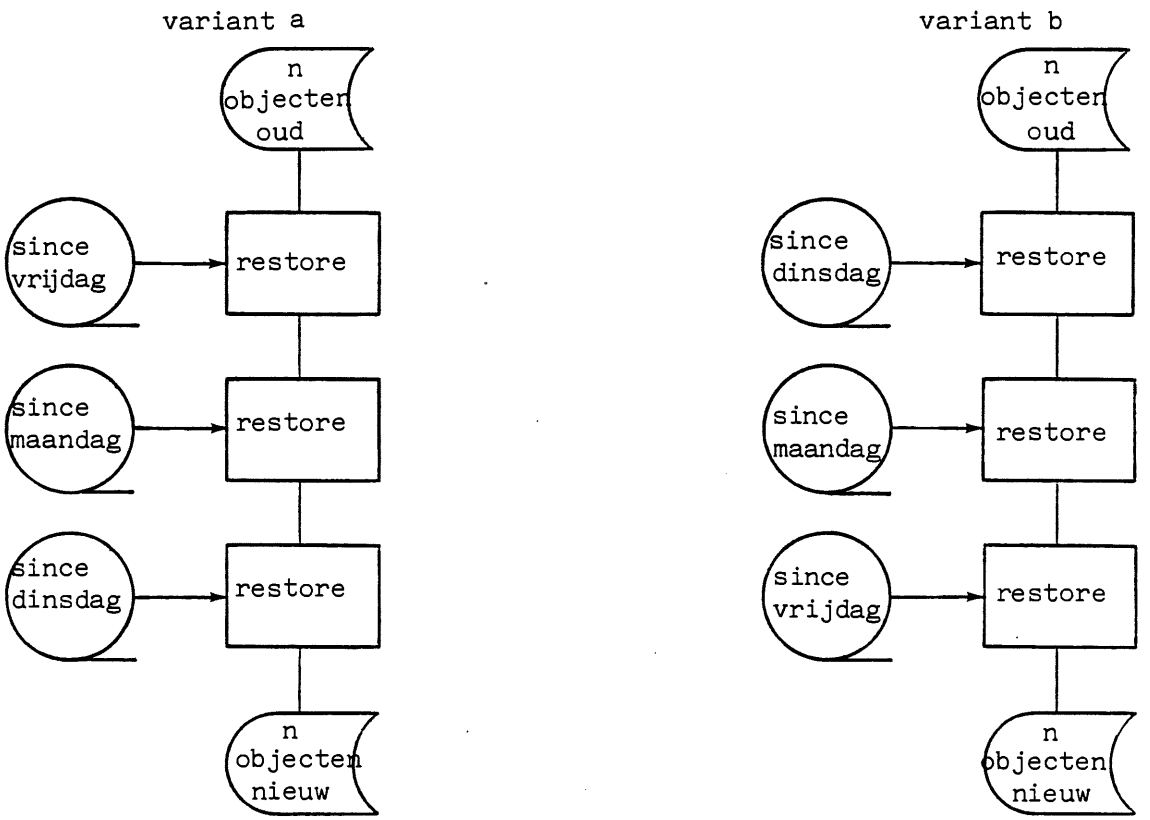
Ingeval van storing worden de gemuteerde objecten in tijdsvolgorde aangebracht op de laatst gemaakte kopie van de informatiedrager.

Variant b

De variant is gelijk aan a met dit verschil dat bij Recovery gestart wordt met de laatst gemaakte since tape en vervolgens terug wordt gewerkt naar de oudste volgend op het tijdstip waarop een volledige kopie is gemaakt van de informatiedrager. De since tape bevat mutaties over een bepaalde periode.

Uit efficiency overwegingen is de variant b te verkiezen boven de variant a. Immers, bestanden op de "since-Vrijdag-tape", kunnen naderhand weer gemuteerd zijn en derhalve voorkomen op een latere "since-tape".
In de variant b wordt teruggewerkt en om deze reden speelt de datumregistratie voor de objecten in de index van de informatiedrager een grote rol. De "since-Dinsdag-tape" bevat de laatste versies van de gemuteerde objecten. Bij het terugzetten van de objecten wordt ook de datum van laatste wijziging weer teruggezet in de index. Zijn er op de "since-tapes" van oudere datum ook objecten welke reeds teruggezet zijn naar het te herstellen medium dan worden deze objecten op grond van de (oudere) datum overgeslagen.

BASIS SITUATIE



Figuur 12.

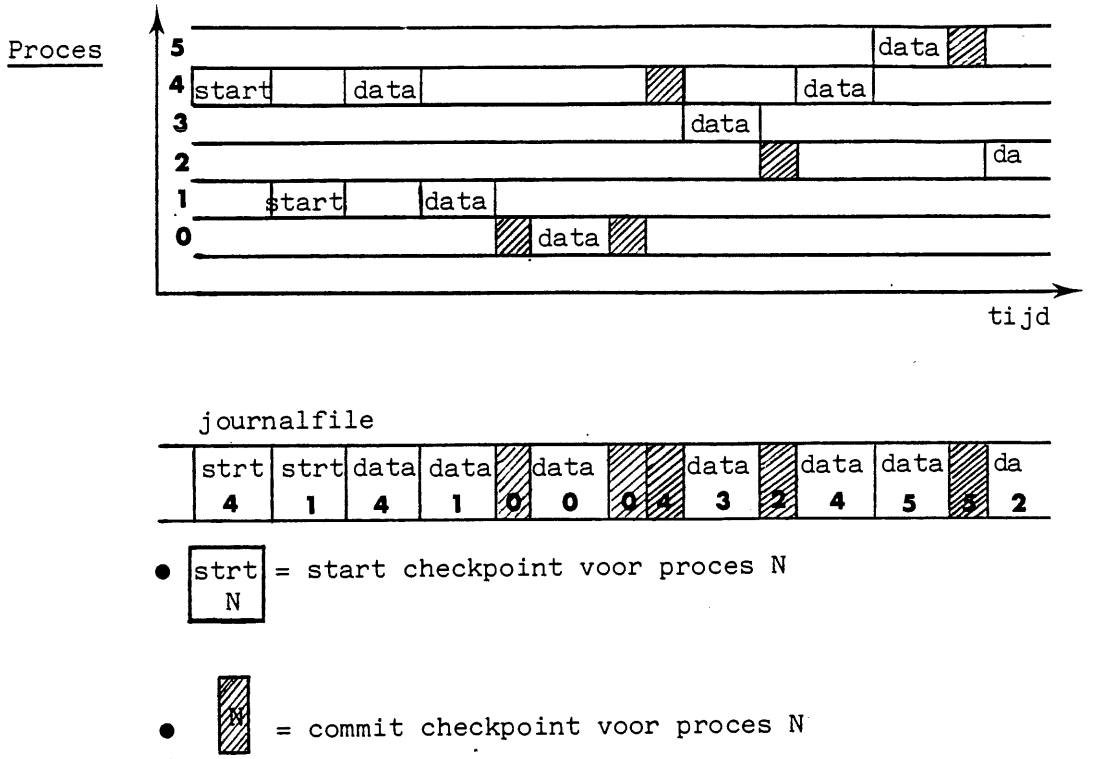
In een real time on-line omgeving wordt gebruik gemaakt van aanvullende (standaard) besturingsprogrammatuur (DBMS, TP-monitor), die technische faciliteiten bieden waardoor het gebruik van back-up kopieën bij de categorie gegevensbestanden niet altijd nodig is. De situatie wordt daardoor wel complexer. Doordat mutaties rechtstreeks op het bestand worden aangebracht, ontbreken de invoerbestanden. Bovendien zijn ingeval van storing de processen niet onder exact gelijke condities en omstandigheden te herhalen.
De standaardprogrammatuur biedt de mogelijkheid (stelt verplicht) gebruik te maken van de logfiles of de journalfiles. Bovendien bevat de standaardprogrammatuur standaard recovery-faciliteiten gebaseerd op het gebruik van logfiles of de journalfiles.
De functies van deze faciliteiten worden bepaald door de inhoud van de log- c.q. journalfile.
Deze logfile kan de volgende informatie bevatten:
1. before en after image;
2. alleen before images;
3. alleen after images;
4. mutaties zelf.

Ad 1.

Terminologie die hierbij ter sprake komt en enigerlei verduidelijking behoeft, is checkpoint, roll backward en roll forward.
Het principe van checkpoint is dat bepaalde informatie wordt weggeschreven op tape/schijf betrekking hebbend op de status van een actief proces (een programma in uitvoering).
Hierbij kan de situatie zich voordoen dat een checkpoint informatie bevat van alle op dat moment actieve processen (een foto van het totale interne geheugen van de machine dus inclusief opdrachtregisters, opdrachttellers, etc.) of informatie per proces.
In het eerste geval wordt ook wel gesproken van een "snap shot". Deze "snap shot" informatie wordt over het algemeen gebruikt door systeemprogrammeurs bij storingen binnen de machine (trouble shooting). Als in dit artikel over checkpoint wordt gesproken wordt de statusinformatie per proces bedoeld.

Er zijn vier soorten checkpoints te onderkennen:
- een start checkpoint, welke altijd en automatisch wordt weggeschreven zodra een programma actief wordt;
- een einde checkpoint, eveneens altijd en automatisch aangebracht zodra een programma normaal beëindigd wordt;
- een commit checkpoint, een in de toepassingsprogrammatuur gedefinieerd checkpoint (dus optioneel);
- een abort checkpoint, een checkpoint dat gegenereerd wordt enerzijds zodra een programma stuk loopt, anderzijds op verzoek van het programma zelf op grond van een zogenaamd "Rollback-statement".

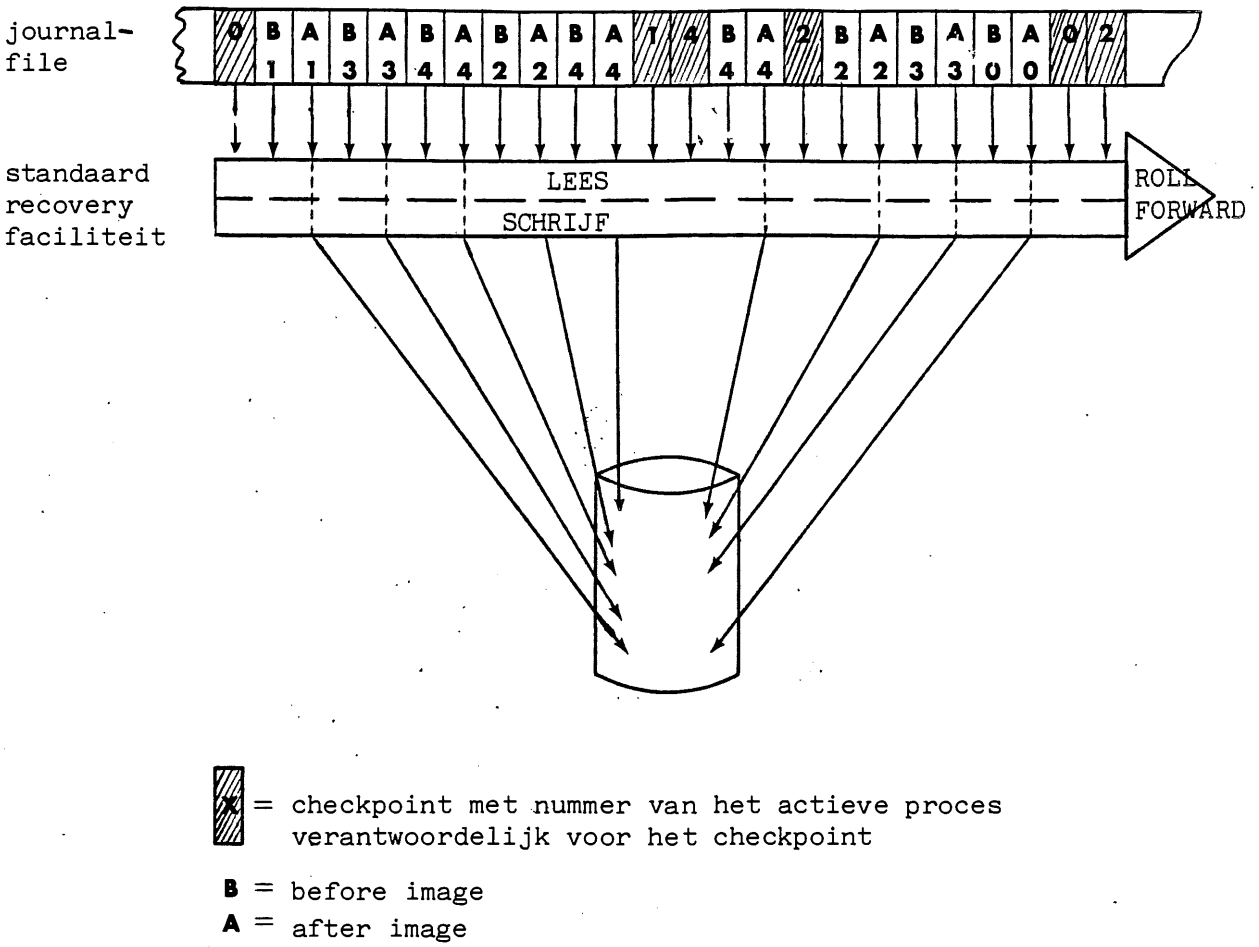
In figuur 13 wordt de volgtijdige inhoud van een journalfile weergegeven ten opzichte van de acties van actieve processen.



Figuur 13. Volgtijdige inhoud van een journalfile.

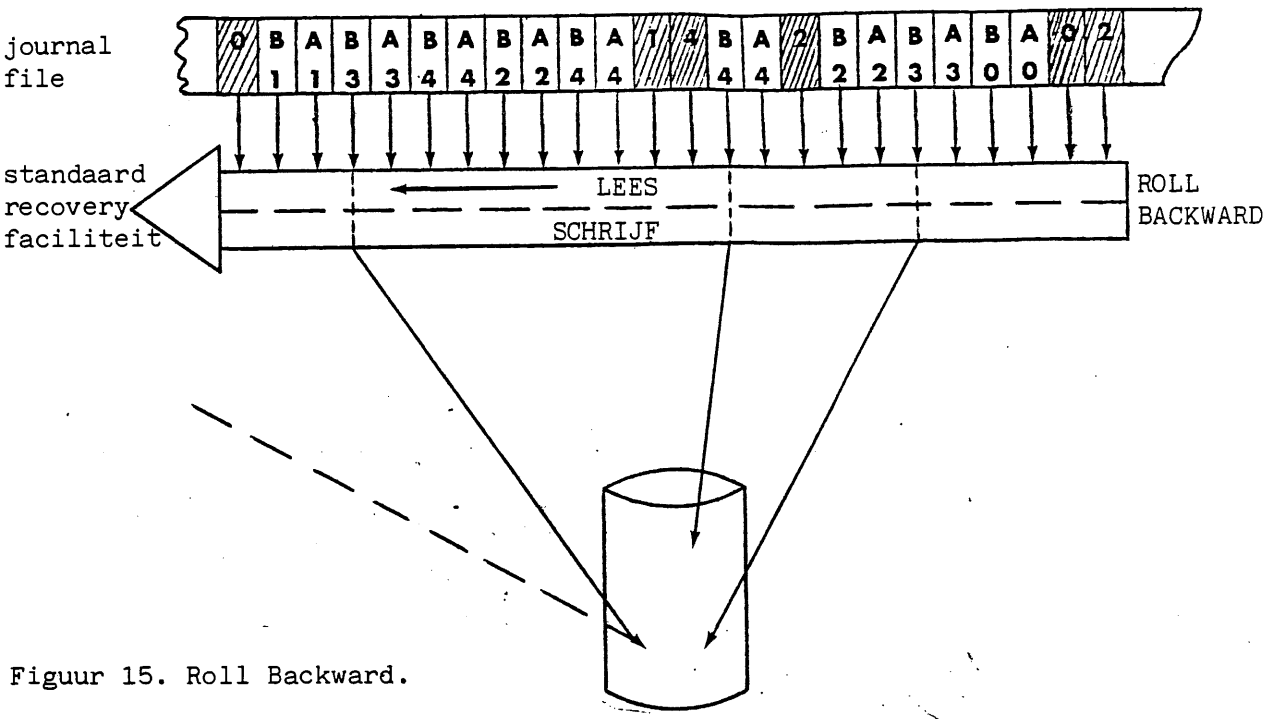
De statusinformatie wordt gebruikt om een verstoord proces (nadat de gegevens hersteld zijn tot op het punt van de checkpoint) te kunnen continueren.

De terminologie van roll forward en roll backward wordt verduidelijkt met behulp van een voorbeeld ingeval van algehele vernietiging van de informatiedrager.
Bij recovery dient dus gebruik gemaakt te worden van een kopie-bestand (zoon). Hierop dienen de verloren gegane mutaties te worden aangebracht. Dit geschiedt met gegevens voorkomend op de journalfile (in casu correcte before en after images).
Het meest efficiënt lijkt direct de after images weg te schrijven naar het kopie-bestand om de situatie ten tijde van de calamiteit te bereiken (echter zoals vaak voorkomt: schijn bedriegt!).
De techniek die op deze wijze de situatie tracht te herstellen wordt "Roll Forward" genoemd (figuur 14).



Figuur 14. Roll Forward.

Als alleen van deze Roll Forward techniek wordt uitgegaan ligt een nieuwe calamiteit in het verschiet. Het proces zal vanwege niet volledig afgewikkelde mutaties abrupt stoppen. Dit wordt ondervangen door het aanroepen van een standaard utility.
Omdat nu onbekend is wat de laatst correct verwerkte mutatie is geweest, wordt teruggekeerd tot het per proces laatst genomen checkpoint. Op deze punten was het bestand inhoudelijk wel correct. De na het checkpoint gemuteerde records moeten teruggebracht worden in de situatie van vóór de wijziging.
Hiervoor gebruikt men de Roll Backward recovery-faciliteit (figuur 15). Deze routine maakt gebruik van de before images (de inhoud van het record vóór de wijziging). Deze routine gaat zover terug met het aanbrengen van before images totdat per proces een checkpoint is aangetroffen.
De gebruikers dienen bericht te ontvangen van de laatst goed verwerkte mutatie. Dit laatste kan grote problemen opleveren als niet op een doordachte wijze is geprogrammeerd. In hoofdstuk 5 wordt hierop nader ingegaan.



Figuur 15. Roll Backward.

Als informatiedragers voor de journalfile worden gebruikt magneetband en magneetschijf.
Voor zover journalfiles op magneetschijf geregistreerd staan is het mogelijk dat met de signalering van een calamiteit door de harde software zonder menselijke tussenkomst Roll Backward uitgevoerd wordt waarna de verwerking opnieuw wordt voortgezet.
Deze herstelprocedure wordt ook wel "Recovery with warm restart" genoemd.
Wordt als medium de magneetband gebruikt dan is menselijke interventie nodig bij het plaatsen/verwisselen van de magneetbanden.
Een automatische restart is niet mogelijk.
Deze herstelprocedure wordt ook wel "Recovery with cold restart" genoemd.

Ad 2. en 3.

Bevat de journalfile alléén before images of alléén after images dan wordt de problematiek alleen maar complexer.
Een Roll Forward alleen leidt niet tot herstel van de situatie vlak voor het optreden van de calamiteit.
Eigen programmatuur zal geschreven moeten worden om de Roll Backward faciliteit in enigerlei wijze te vervangen.
Het probleem is de vaststelling van de laatst correct verwerkte mutatie per proces.
Bij een Roll Backward, waarbij slechts after images beschikbaar zijn, moet bedacht worden dat - aangekomen op de checkpoints - de direct na een checkpoint komende mutatie reeds verwerkt kan zijn.
Ook hier zal speciale programmatuur aanwezig moeten zijn om de laatst verwerkte mutatie te detecteren.

Ad 4.

Voor zover de logfile of de journalfile de mutaties zelf bevat, moeten uitgaande van de laatst genomen kopie van het gegevensbestand, de verwerkingsprocessen worden herhaald. Deze situatie komt echter zelden voor.
Wat wel voorkomt is dat de mutaties zelf deel uitmaken van het gegevensbestand en opgeslagen worden in een deelgebied van dat bestand. Dit wordt gedaan om een tweetal redenen. Enerzijds kunnen nu mutatieverslagen worden gecreëerd anderzijds kan het aantal journalfiles (in de tijd gezien) worden beperkt.

Tot slot wordt ingegaan op de situatie waarbij de calamiteit de informatiedrager treft. Deze kan de journalfile al of niet in combinatie met het gegevensbestand zelf bevatten.
Ingeval alleen de journalfile verloren is gegaan is er theoretisch nog niets aan de hand. Immers de gegevensverwerking kan gecontinueerd worden.
Zijn zowel de journalfile als het gegevensbestand betrokken bij de calamiteit dan zit er veelal niets anders op dan alle mutaties opnieuw in te brengen vanaf het tijdstip van de laatst genomen kopie.

In hoofdstuk 3 is uitgebreid ingegaan op Back-up; in dit hoofdstuk op Recovery en Restart.
De behandeling van de problematiek is tot nu toe niet uitputtend geweest. Dit is ook niet mogelijk door de aanwezigheid van specifieke aspecten, welke grote invloed hebben op de complexiteit als geheel.
Enkele van deze specifieke aspecten worden in het hierna volgend hoofdstuk nader besproken.

5. Specifieke aspecten

A. Besturingssysteem en overige harde software (utilities)

Het besturingssysteem is over het algemeen ondergebracht op een verwisselbare magneetschijf (Eng.: Removable pack, Removable disk). Raakt de schijf in het ongerede als gevolg van een calamiteit dan is na schijfwisseling de machine weer beschikbaar voor produktie.
De laatste tijd komt het gebruik van vaste schijven (snellere toegangstijd, grotere opslagcapaciteit) steeds meer in zwang. Dit heeft tot gevolg dat, indien deze schijf door een calamiteit onbruikbaar wordt, het besturingssysteem niet meer benaderbaar is. In deze gevallen zal een nieuwe systeemgeneratie moeten worden uitgevoerd met uitwijk naar een andere schijfveneenheid.
Om bovenstaande reden is het aan te bevelen het besturingssysteem altijd aan te brengen op een verwisselbare magneetschijf.

B. Gegevensbestanden

1. Logfile en/of journalfile kunnen in eerste instantie worden opgeslagen op een schijfgeheugen. In deze situatie is aandacht nodig voor het "wrap around" mechanisme hetgeen inhoudt dat als de bestandsruimte volgeschreven is, het systeem weer aan het begin van de bestandsruimte begint te registreren en daarmede oude mutaties overschrijft.
   In het besturingssysteem (of DBMS-software) dienen waarborgen te zijn opgenomen, welke het hiervoor aangegeven risico uitsluiten door periodiek te waarschuwen zodra bepaalde grenzen worden overschreden respectievelijk de verwerking te staken indien de bestandsruimte vol en geen andere vrije ruimte beschikbaar is.
   De verwerking mag pas worden voortgezet nadat de inhoud is gekopieerd op bijvoorbeeld een magneetband.
   Logfile en/of journalfile worden ook veelvuldig direct weggeschreven naar magneetband(en).
   Ook hier dient het besturingssysteem (of DBMS-software) te waarschuwen (en indien geen ander medium beschikbaar is, de verwerking te staken) indien de magneetband is volgeschreven.
   Dit om geen mutaties te verliezen.

2. Wordt bij geïntegreerde verwerking geen gebruik gemaakt van DBMS- software en staat het systeem naast real time on-line-verwerking ook batch-verwerking toe, dan kan niet zonder meer voor herstel van het bestand gebruik gemaakt worden van de logfile of de journalfile, aangezien de invloed van de batch-mutaties op ook middels real time on-line gewijzigde records niet bekend is.
   Herhaald wordt het reeds in hoofdstuk 4 gestelde "dat de processen niet onder exact gelijke condities en omstandigheden te herhalen zijn".
   Er zijn DBMS-systemen waarbij ook het batch-proces als een real time systeem gedefinieerd kan worden. In dit geval worden ook de batch-mutaties weggeschreven naar de journalfile en vervalt het hiervoren beschreven voorbehoud.

3. Met betrekking tot de recovery-problematiek bestaat een probleem als gevolg van het mogelijk niet synchroon lopen van log- c.q. journalfile.
   Ingeval gebruik wordt gemaakt van locale databases in combinatie met een centrale database moeten de mutaties in de locale databases ook terug te vinden zijn in de centrale database.
   Elke database heeft haar eigen journalfile. Is de gezamenlijke inhoudelijke waarde van de mutaties op de "locale journalfiles" gelijk aan de inhoudelijke waarde van de journalfile van de centrale database?

   In een configuratie waarbij meerdere processoren de aangeboden jobs (processen) verwerken geldt een synchronisatieprobleem van andere orde. Hoe wordt de registratie op de journalfiles uitgevoerd? Door één of door elke processor afzonderlijk? Indien dit gebeurt door één processor is volledigheid gewaarborgd.

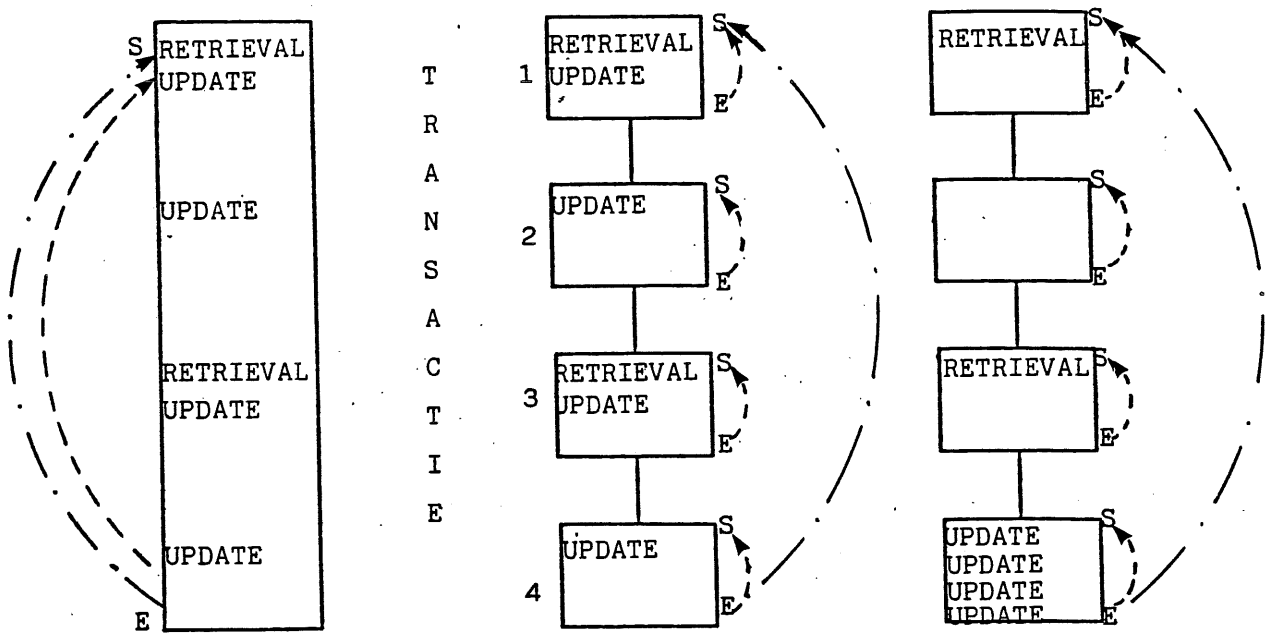
Voor zover mutaties twee keer geregistreerd worden op gescheiden log- en/of journalfiles (het zogenaamde dual-logging system) kan de vraag gesteld worden: of de log- en/of journalfiles qua inhoud en volgorde identiek zijn (tijdverschillen in registratie!).
De problematiek wordt complexer naarmate er meerdere processoren aanwezig zijn voor de gegevensverwerking.
Dit kan uit recovery-oogpunt problemen opleveren als geen aandacht is geschonken aan de synchronisatie van de processen en de synchronisatie in de volgtijdelijkheid van de before en after images op de logfiles (journalfiles).

In dit hoofdstuk zijn tot dus verre kort een aantal specifieke aspecten behandeld welke de problematiek inzake recovery en restart complexer maken.
De problemen zijn in vele gevallen door de computerleveranciers onderkend waardoor software beschikbaar is om de problemen te voorkomen. Daarnaast zal de oplossing gevonden moeten worden in organisatorische maatregelen en procedures.
Hierna zal kort worden ingegaan op de invloed van de programmeerwijze op het recovery- en restartproces.

C. Conversationeel/pseudoconversationeel programmeren en de invloed hiervan op het recovery- en restartproces

In hoofdstuk 4 is bij de verduidelijking van de begrippen roll forward en roll backward gesteld dat gebruikers - na herstel - een bericht dienen te ontvangen van de laatst goed verwerkte mutatie.
En dat was dan dat!
Als echter niet op doordachte wijze is geprogrammeerd dan is dit doorgeven van de laatst goed verwerkte mutatie moeilijk realiseerbaar.
Een voorbeeld maakt dit duidelijk. Daarbij is het nodig dat de aard van een tweetal programmeringstechnieken nader worden beschreven.
Bij conversationeel programmeren wordt alle coding behorende tot één transactie in één groot programma ondergebracht in tegenstelling tot pseudo-conversationeel waar de coding is "verknipt" tot kleinere logische eenheden ter verhoging van de efficiency van het computersysteem.
De processor van het computersysteem ziet zowel het "grote" programma als de "kleine" logische eenheden als aparte processen en handelt daar ook naar door het genereren van de respectievelijke checkpoints (start, einde en abort); zie voor een schematische weergave figuur 16.

Orderverwerking.



------ transactie voor het computersysteem
-.-.-. transactie voor de gebruiker
S - Start checkpoint
E - Einde checkpoint

Figuur 16.

Stel bijvoorbeeld een orderverwerkingsproces waarbij zowel afnemergegevens ten aanzien van het totaal orderbedrag, ordergegevens als artikelgegevens ten aanzien van bestelde aantallen e.d. worden bijgewerkt.

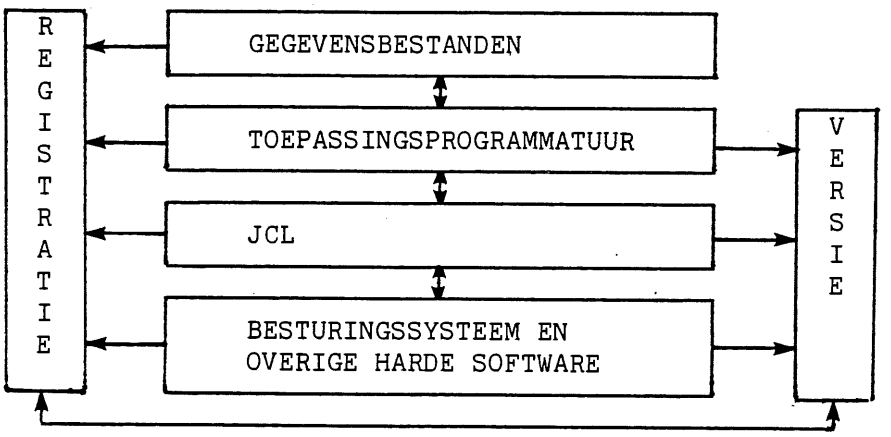
De gebruiker heeft geen idee wanneer effectief gegevens worden bijgewerkt en kent slechts de order behorende bij een bepaalde afnemer.
Als er iets fout gegaan is in de verwerking verwacht de gebruiker dat het systeem de laatste goed verwerkte order meldt.
Het systeem keert terug zoals beschreven is in hoofdstuk 4 tot het start-checkpoint van een proces en is zoals in het middendeel van figuur 16 is weergegeven niet in staat terug te keren tot het begin van de totale transactie.
De transactie is deels verwerkt; de gebruiker weet niet welk deel!
De integriteit van de gegevens is niet meer gewaarborgd.
De oplossing hiervoor is dat alle wijzigingen op de gegevens zolang mogelijk worden tegengehouden en worden doorgeschoven tot het laatste "logische" deel alwaar dan de eigenlijke wijzigingen effectief worden gemaakt.

6. Controle-implicaties

In voorgaande hoofdstukken is uiteengezet "wat" er bij back-up, recovery en restart zoal komt kijken. Daarbij heeft de schrijver zich beperkt tot beschrijvende zaken. In dit hoofdstuk wordt ingegaan op een aantal controle-implicaties die back-up, recovery en restart met zich brengen. Die controle-implicaties zijn gericht op de continuïteit van de geautomatiseerde gegevensverwerking. Anders gezegd: waaraan dient aandacht te worden besteed uit oogpunt van continuïteit?

1. Procedures en voorschriften

Binnen de automatiseringsorganisatie zijn meestal één of meerdere procedures aanwezig waarin wordt aangegeven, welke acties ondernomen moeten worden om de continuïteit van de gegevensverwerking ingeval van calamiteiten/storingen in redelijke mate te waarborgen. Meestal zijn deze onvolledig en slechts gericht op de beveiliging van gegevens. Bovendien worden procedures niet aangepast aan veranderende (complexe) situaties. Om de continuïteit van de gegevensverwerking in redelijke mate te kunnen waarborgen dienen binnen de back-up-, recovery- en restart-procedures aandacht besteed te worden aan de vier categorieën besturingssysteem, programmatuur, JCL en gegevensbestanden alsmede de daarbij behorende bestandsregistraties. (In figuur 17 is de relatie welke bestaat tussen de categorieën schematisch weergegeven.) In het voorgaande is niet over deze registratie gesproken; zij is echter wel van eminent belang. In 6.3 wordt nader op het belang van de registratie ingegaan.
Een ander aspect dat in dit kader de aandacht verdient is de naleving van de procedures en voorschriften gericht op de continuïteit. De praktijk wijst uit dat er meestal wel procedures en voorschriften bestaan doch dat deze niet worden aangepast aan veranderende omstandigheden. Dit blijkt meestal uit het feit dat controle op de naleving van bestaande procedures niet wordt uitgevoerd. Als dit wel het geval is dan worden veranderde situaties eerder onderkend hetgeen dan aanpassing van de procedures tot gevolg heeft. Dit is echter geen ideale situatie.



Figuur 17.

Het is aan te bevelen binnen de automatiseringsorganisatie een functie te creëren die verantwoordelijk is voor de beveiligingsaspecten in brede zin. Deze dient op de hoogte te zijn van veranderingen die in apparatuur en programmatuur uit hoofde van beveiliging consequenties met zich brengen en derhalve zorg te dragen voor aanpassing alsmede naleving van procedures. Hier vallen back-up-, recovery- en restart-procedures ook onder.

2.A Besturingssysteem en overige harde software

Bij het besturingssysteem kunnen zich een aantal complicaties voordoen.
Een besturingssysteem wordt door de leverancier geleverd. Hierop wordt, evenals op andere programmatuur, onderhoud gepleegd.
Wijzigingen (PTF's) worden eveneens door de leverancier geleverd.
Welke van die wijzigingen worden aangebracht is per situatie verschillend.
Daarnaast kunnen door de eigen organisatie wijzigingen c.q. aanvullingen (o.a. patches) worden aangebracht. Uit continuïteitsoverwegingen zijn een aantal situaties te onderkennen.

1. de meest ideale is dat alleen gebruik wordt gemaakt van het ongewijzigde besturingssysteem van de leverancier zonder eigen wijzigingen/aanvullingen (dit impliceert dat ook alle wijzigingen van de leverancier (PTF's) worden aangebracht.
   In geval van een calamiteit kan altijd worden teruggevallen op de leverancier.

2. minder ideaal wordt het als gebruik wordt gemaakt van het standaard besturingssysteem zonder eigen wijzigingen doch met een selectie uit de PTF's.
   Terugvallen op de leverancier wordt dan moeilijker tenzij bekend is welke selectie is gemaakt uit welke wijzigingen. Hierbij komt tevens het probleem dat de wijzigingen van de leverancier voorzien zijn van versienummering (release).
   In dit geval is het raadzaam na het aanbrengen van veranderingen een kopie van het bestand te maken.
   Bovendien is registratie noodzakelijk van de plaats waar de kopie van het bestand wordt bewaard. (Dit is meestal niet het geval.)

3. in het laatste geval worden op het besturingssysteem van de leverancier (inclusief alle of een selectie uit de PTF's) eigen wijzigingen/aanvullingen aangebracht.
   Terugvallen op de leverancier is ingeval van een calamiteit bijna niet mogelijk.
   De oplossing voor het continuïteitsprobleem moet binnen de automatiseringsorganisatie zelf worden gevonden.
   Kopieën van het besturingssysteem inclusief alle daarop aangebrachte wijzigingen, dienen aanwezig te zijn.
   Het volledigheidsaspect van eigen wijzigingen verdient aandacht evenals de registratie van locaties waar bestanden zich bevinden.

Beklemtoond dient te worden dat, indien in de gevallen 2 en 3 geen kopieën worden gemaakt van de mutaties, de registratie zéér belangrijk is.
Indien de registratie handmatig plaatsvindt, is aan te bevelen deze in duplo te voeren en gescheiden op te slaan.

2.B Toepassingsprogrammatuur (source-coding)

Over het algemeen levert deze categorie niet zoveel problemen op als na het aanbrengen van mutaties in de produktie-omgeving twee kopieën worden getrokken welke gescheiden worden opgeslagen. Dit dient te geschieden direct na het aanbrengen van de wijziging. Wordt dit niet direct gedaan doch met een vaste periodiciteit dan kan het voorkomen dat, indien teruggevallen moet worden op back-up kopieën, met verouderde programmaversies wordt gewerkt.
De back-up procedure dient er in te voorzien dat, alvorens produktie wordt gedraaid, de tussentijds geëffectueerde wijzigingen wederom worden aangebracht.

2.C Job Control Language

Deze categorie krijgt in het kader van de continuïteit vrijwel geen aandacht en komt in de back-up procedures niet voor. Toch is deze categorie belangrijk en wel met betrekking tot het volgtijdig gebruik van gegevensbestanden (in casu de versies van de bestanden). Als van alle overige categorieën kopieën, etc. beschikbaar zijn en de JCL ontbreekt dan is produktie niet mogelijk.
De reproduktietijd van de JCL dient niet te worden onderschat. De reproduktie is in het geheel niet mogelijk als geen documentatie wordt bijgehouden. In het kader van de back-up en recovery dient aan de documentatie van de JCL derhalve aandacht te worden besteed.

2.D Gegevensbestanden

Deze categorie krijgt in het kader van continuïteit altijd de meeste aandacht.
Als over back-up, recovery en restart procedures wordt gesproken wordt meestal alleen aan deze categorie gedacht.
Er bestaat, als over gegevensbestanden wordt gesproken, de neiging alleen te denken aan stam- en mutatiebestanden en niet aan bestanden die met een speciale naam worden aangeduid (bijvoorbeeld journal-files). Dergelijke gegevensbestanden behoren eveneens aandacht te krijgen in de back-up en recovery procedure.

Het verdient aanbeveling de opslag zodanig te regelen dat generatie-versies met de daarop aansluitende mutatiebestanden bij elkaar worden gearchiveerd.
Bovendien dienen identieke bewaartermijnen in acht te worden genomen bij bestanden welke invloed op elkaar uitoefenen.

3. Registratie van bestanden

In het voorgaande is herhaaldelijk gesproken over registratie van bestanden.
Alhoewel deze registratie voor de continuïteit van groot belang is, krijgt zij niet de aandacht die zij eigenlijk zou moeten hebben. Immers als van alle categorieën back-up kopieën beschikbaar zijn doch niet bekend is waar zij zich bevinden dan is in geval van calamiteit de continuïteit van de gegevensverwerking niet gewaarborgd.

Benadrukt moet worden dat om een drietal redenen de registratie aandacht verdient.

1. Zoals hierboven is aangegeven is registratie noodzakelijk om aan te geven waar welke bestanden zich op welk moment bevinden. Wellicht is het overbodig te vermelden dat de registratie up-to-date moet zijn.

2. De registratie dient zelf beveiligd te worden en dient derhalve de aandacht te hebben bij het opstellen van back-up en recovery-procedures. In de praktijk komen zowel handmatige als geautomatiseerde registraties voor.
   In het eerste geval dienen stringente maatregelen te worden getroffen dat die handmatige registratie op een beveiligde (brandvrije, hittebestendige) plaats wordt bewaard. Dit vanwege het feit dat het praktisch ondoenlijk is de registratie in duplo te voeren en de kopie elders te bewaren. Als de registratie is geautomatiseerd dan valt de registratie onder de categorieën "programmatuur" en "gegevensbestanden".
   Zij dienen dan ook onder de desbetreffende back-up en recovery-procedures te vallen.

3. Last but not least het controle-aspect dat aan registratie kan worden ontleend.
   Door middel van de registratie kan de naleving van voorschriften en procedures worden gecontroleerd. Een probaat middel is het periodiek inventariseren van de inhoud van de opslaglocaties. Tevens kan de beweging worden gecontroleerd van de gegevensbestanden tussen de locaties.
   Voor het uitvoeren van deze inventarisatie is geen automatiseringskennis vereist. Tapes en schijven zijn herkenbaar aan externe labels die dienen voor te komen op de registratie zelf. Ingewikkeldheid dient te worden vermeden omdat het ingeval van calamiteit tot grote problemen aanleiding kan geven.

4. Bruikbaarheid van back-up kopieën

Als voldaan is aan alle aspecten genoemd in voorgaande hoofdstukken en paragrafen, zou de indruk kunnen ontstaan dat rustig kan worden geslapen en er niets meer valt te vrezen. Ook hier levert de techniek haar bijdrage tot het ongewisse.
Immers hoe wordt vastgesteld dat de produktie van back-up kopieën feilloos is verlopen?
Op welke manier wordt gecontroleerd of de back-up kopieën als zij gebruikt moeten worden te lezen zijn? Meestal wordt aangenomen dat bij het maken van deze kopieën de techniek feilloos heeft gewerkt.
Aan te bevelen is om aangemaakte kopieën terug te lezen of althans een steekproef hierop te houden.
Dit om onaangename verrassingen in toch al penibele situaties zoveel mogelijk te vermijden.

Tenslotte

Getracht is in dit artikel een tip van de sluier op te lichten die er naar de mening van de auteur hangt over de complexe problematiek van back-up en recovery. Een poging is gedaan om de zaken op een rij te zetten en de lezer een indruk te geven van voornoemde complexiteit en bovendien diegenen de helpende hand te bieden die in de praktijk uit hoofde van hun beroepsuitoefening geconfronteerd worden met deze problematiek.
Daarnaast is getracht aan te geven waaraan aandacht moet worden besteed indien een oordeel moet worden gegeven over hoe het gesteld is met de continuïteit van de gegevensverwerking ingeval van calamiteit.

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

PASSWORD-PROTECTIE

door A. van der Drift

1. Inleiding

In de journalistiek doet de automatisering duidelijk zijn intrede niet alleen door de automatiseringsondersteuning voor de totstandkoming van onder meer dagbladen, maar ook doordat er over geschreven wordt.
Het schrijven richt zich ditmaal niet zozeer op de techniek of op de werkeloosheid die automatisering ten gevolge heeft maar heden ten dage meer nadrukkelijk juist op het spektakel. Wat is immers meer spectaculair dan "criminaliteit"; bankinbraken per home-computer of atoomoorlogje door verbindingen tussen deze computers en de Pentagon-apparatuur!
Hieraan wordt heel wat publiciteit gegeven. "Adviseurs" terzake verdienen er weer forse boterhammen mee; de filmindustrie speelt hier aardig op in.
Kortom er zou bijna sprake kunnen zijn van een "mode"-verschijnsel onder de naam van "Crime by Home-Computer".

Om de indruk uit menig persbericht ietwat te relativeren volgt een korte uiteenzetting over het samenspel tussen techniek en organisatie in het kader van password-protectie; een beveiliging die gebaseerd is op een geautomatiseerde herkenning van een persoon door de wachtwoordcontrole, aan de hand waarvan de bevoegdheden worden vastgesteld door de beveiligingsprogrammatuur.

2. Techniek en organisatie

De computerbeveiliging stoelt op twee hoofdpeilers:
- de techniek of technische ondersteuning;
- de organisatie en de daarin bestaande procedures en voorschriften.

Een simpele kluis dient hier als voorbeeld. De techniek wordt onder meer gevormd door de moeilijk doordringbare wanden alsmede het veelal geavanceerde slot.
De organisatie daaromheen wordt onder meer gevormd door de beperkte uitgifte van sleutels, de locatie van de kluis alsmede bijvoorbeeld de integriteit van de desbetreffende slotenmaker om geen kopie-sleutels achter te houden.
Bedenk echter dat geen slot perfect is; er bestaan immers "spectaculaire" meesterkrakers.

Analoog met het kluisvoorbeeld wordt bij geprogrammeerde toegangsbeveiliging de techniek gevormd door de beveiligingsprogrammatuur, de sleutel door het password en de organisatie door de wijze waarop deze programmatuur wordt gebruikt, de omgeving waarin deze programmatuur actief is alsmede de integriteit van de bouwer(s).

Bedenk ook hierbij dat (nog los gezien van gewone programmafouten) geen beveiligingsprogramma perfect is; er blijken immers "spectaculaire" meesterkrakers of zelfs krakertjes te bestaan.

Er zullen adequate organisatorische maatregelen dienen te worden getroffen teneinde elk risico zo veel mogelijk te beperken. Zo ook zullen er adequate technische ondersteuningen door beveiligingsprogrammatuur moeten worden geboden ten einde voortdurend ongeautoriseerde ingrepen te voorkomen.

3. Betekenis passwords

Een password heeft primair en veelal louter en alleen tot doel de beveiligingsprogrammatuur een mogelijkheid te bieden voor het vaststellen van de authenticiteit van de persoon, die in verbinding staat met de computer (middels een terminal).
Bijna altijd heeft men de beschikking over een toetsenbord, waarop het password desgevraagd kan worden ingetoetst.
Indien men de beschikking heeft over stem-, handschrift- of vingerafdruk-herkenningsapparatuur, gebruikt men dienovereenkomstige "passwords".
(Zou men een "algemeen" password willen invoeren ten behoeve van de continuïteit in geval van een onvoorziene afwezigheid van de gebruiker, dan kan men ook op deze geavanceerde apparatuur de vindingrijkheid botvieren. Denk bijvoorbeeld aan cassette-opname van stemgeluiden, simpele lijnen met behulp van een lineaal of handschoenafdrukken. Het zij echter toegegeven dat gebruik van dergelijke apparatuur de beveiliging ten goede kan komen, maar getuige de voorbeelden nog steeds in combinatie met adequate organisatorische maatregelen.)

4. Effectiviteit passwords

Ten behoeve van de gebruikers van passwords kunnen de navolgende eisen worden genoemd:
- kies geen algemeen voor de hand liggende passwords zoals initialen, e.d.;
- kies passwords met verschillende en meerdere tekens (bijvoorbeeld 5 tot 8 alfanumerieke tekens);
- houdt het password geheim en wijzig het frequent.

De navolgende ondersteuning van voornoemde eisen zou door de beveiligingsprogrammatuur kunnen worden geboden:
- accepteer geen passwords, die ouder zijn dan bijvoorbeeld 6 weken;
- accepteer geen passwords van identieke en/of minder dan vijf tekens;
- accepteer geen nieuwe passwords, die recentelijk reeds eerder zijn gebruikt.

5. Gebruik passwords

De volgende faciliteiten zouden door beveiligingsprogrammatuur kunnen worden geboden:
- maak een password nooit zichtbaar, noch op papier, noch op de terminal;
- sla de passwords versluierd (encrypted) op en/of beveilig de toegang tot deze opslag;
- accepteer geen initieel toegekende passwords; dwing eerst een wijziging af door de eigenaar;
- accepteer maximaal 3 pogingen tot het goed invoeren van het password per persoonsidentificatie. Log de foutieve pogingen met vermelding van persoonsidentificatie, terminalidentificatie, datum en tijd. Geef een duidelijk signaal van overschrijding aan standby computerpersoneel.
  Koppel zo mogelijk bij overschrijding de verbindingslijn af, totdat geautoriseerd computerpersoneel dit herstelt;
- ondersteun zo nodig dubbele aanlog-procedures (aanmeldprocedures) vanaf meer dan één terminal;
- laat de terminal vermelden wie aan- en aflogd en zo mogelijk wanneer de persoon voor het laatst heeft aangelogd.

De eisen in dit verband zijn:
- beveilig de versluieringsberekening;
- beveilig fysiek de computerbestanden, waarop de passwords kunnen zijn vastgelegd (ook de back-up files);
- creëer zo nodig een aanlog-procedure bestaande uit twee gescheiden onderdelen;
- onderneem zo mogelijk direct actie op signalen betreffende het overschreden aantal pogingen.

6. Aanvullende maatregelen

De navolgende additionele faciliteiten zouden door beveiligingsprogrammatuur kunnen worden geboden:
- forceer een automatische log-off (afmelding gebruiker) na een bepaalde tijd waarin de persoon op de terminal niet actief is geweest;
- stel personen uitsluitend in de gelegenheid te communiceren met de computer op bepaalde uren van de dag met behulp van bepaalde door de beveiligingsprogrammatuur fysiek te herkennen terminals;
- accepteer geen actieve "applicatie-"programmatuur in het computergeheugen, die niet volgens de voorgeschreven toegangsregels in directe verbinding staat met een fysiek aangesloten terminal, die aanstaat.

Belangrijke organisatorische maatregelen zijn:
- het steeds uitschakelen van de terminal en pas aanzetten als men daadwerkelijk gaat communiceren met de computer;
- het eventueel fysiek beveiligen van de terminal.

7. Uitgifte passwords en beheer beveiligingsprogrammatuur

In de organisatie dienen procedures te bestaan en te worden nageleefd voor wat betreft:

- het verkrijgen van een persoonsidentificatie en initieel password;
- het herkrijgen van een door de eigenaar vergeten password door bijvoorbeeld het wederom verkrijgen van een nieuw initieel password of het toepassen van een envelopprocedure (het noteren van het actuele password en deze notitie deponeren in een gesloten envelop bij de direct hogere chef);
- het beveiligen van de beveiligingsprogrammatuur al dan niet met behulp van (andere) beveiligingsprogrammatuur;
- het verwijderen van de persoonsidentificatie en het password uit de computer, indien iemand wordt overgeplaatst of het bedrijf verlaat.
- het aanpassen van bevoegdheidsprofielen ingeval van wijzigingen in de organisatie.

8. Slot

De genoemde technische en organisatorische maatregelen zullen nauwelijks of niet allemaal binnen één omgeving worden aangetroffen. Dit is ook niet direct noodzakelijk, omdat enkele maatregelen compenserend werken voor de anderen.
Zo ook zal niet in elke organisatie een zo grote noodzaak tot optimale beveiliging door middel van password-protectie aanwezig zijn.
Tevens bieden lang niet alle beveiligingsprogramma's de genoemde faciliteiten en zal niet elke organisatie de discipline voor het naleven van de voorgestelde organisatorische maatregelen kunnen opbrengen, danwel geen controle op de naleving van genoemde maatregelen adequaat kunnen uitvoeren.
Overigens zij opgemerkt dat niet alle maatregelen terzake zijn vermeld. "No program (lees ook: procedure) is perfect".
Lezen wij echter de in de inleiding genoemde "spectaculaire" persberichten, dan kan per bericht geconstateerd worden, dat niet aan ten minste één van de, in die specifieke situatie relevante, genoemde maatregelen is voldaan.

De eerlijkheid gebiedt te vermelden dat de genoemde berichten ten minste één positieve functie vervullen.
Zij vestigen de aandacht op de noodzaak van geprogrammeerde toegangsbeveiliging voor wat betreft het onderdeel password-protectie.

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

REACTIE VAN LEZERS

Onderwerp Password-protectie in Compact herfst 1983 pagina's 19 en volgende, nummer 33 10e jaargang

Geachte schrijver,
Uw artikel heb ik met aandacht gelezen. Het is een indrukwekkende lijst van elkaar aanvullende beveiligingsmaatregelen. Bovendien bijeengebracht in een kort bestek.

Met deze kennis gewapend neem ik het standaard controleprogramma van cliënt X ter hand.
Mijn opdracht luidt:
- beoordeel de interne controlemaatregelen;
- toets deze op hun bestaan en werking;
- pas een cijferbeoordeling toe met aanvullende steekproef naar de massa, opdat een fraude, veroorzaakt door een omissie, die het beeld van de jaarrekening beïnvloedt door mij kan worden getraceerd.

Vraag: Welke opeenvolgende stappen moeten we aanhouden om een goed gebruik van passwords te constateren, ook in het computercentrum.
Neem aan dat alle overige interne en externe controlemaatregelen adequaat zijn genomen en ook adequaat werken.
H.J.M. van der Wielen

Antwoord van de schrijver
Mijn artikel uit de vorige editie van Compact zou meer volledig en toepasbaar zijn met het antwoord op de door u gestelde vraag.
Vandaar dat ik deze kans gaarne benut voor het completeren van voornoemd artikel.

In het algemeen kan worden gesteld dat de controle op de naleving van maatregelen ten aanzien van password-protectie ten nauwste bepaald wordt door de mogelijkheden, die worden geboden door de password-protectie-software. Veelal zullen wij daardoor voor beperkingen worden gesteld.
Een en ander betekent dat de accountant (EDP-auditor) op de eerste plaats bekend dient te zijn met de mogelijkheden en onmogelijkheden van deze software. Hij zal, zonder de software op dit punt ter discussie te stellen, niet meer kunnen verlangen dan datgene, dat door deze software kan worden geboden.
Het kan overigens voorkomen dat installatie-opties invloed uitoefenen op de toepassing van password-protectie, waardoor deze opties object van controle dienen te zijn. In mijn vorige artikel werd hiervan geabstraheerd, zodat ik hier nu niet verder op zal ingaan.
Aan de hand van de punten, genoemd in de hoofdstukken 4 tot en met 7 van het artikel, zal ik mogelijkheden aandragen voor genoemde controle.

Hoofdstuk 4. Effectiviteit passwords

Indien de accountant kan beschikken over een betrouwbare lijst van bij de cliënt in gebruik zijnde passwords met vermelding van de desbetreffende gebruikers en vervolgens een periode later de beschikking kan krijgen over een nieuwe lijst, kan hij de volgende controles verrichten:

- stel vast dat de passwords per gebruiker gewijzigd zijn;
- beoordeel de passwords op willekeurigheid (geen verklaarbare passwords, die andere gebruikers zouden kunnen kennen).

Het verkrijgen van de genoemde lijst is (hoe prettig ook voor onze controle) op zichzelf een vervelende situatie, omdat wellicht ook anderen deze lijst zouden kunnen verkrijgen. Dit zou betekenen, dat wij moeten vaststellen, of anderen deze lijst niet kunnen vervaardigen.
Over de betrouwbaarheid van de verkregen lijst alsmede de effectiviteit van de password-protectie kan onder meer door testen een indruk worden opgedaan.
Indien wij niet over deze lijst kunnen beschikken, blijven er geen andere controlemaatregelen over om voornoemde controle uit te voeren, anders dan datgene dat bij toeval kan worden vastgesteld.
Het kan voorkomen dat de cliënt zo'n lijst niet aan de accountant ter beschikking wil stellen; om begrijpelijke redenen overigens. In deze situatie valt slechts te constateren, dat bij de cliënt voorzichtigheid wordt betracht, hetgeen wij (in beperkte mate) zullen moeten toejuichen.

Op de diverse werklocaties bij de cliënt zou de accountant een indruk kunnen opdoen over het geheim houden van passwords (geen stickers met passwords op de terminals, etc.).

Hoofdstuk 5. Gebruik passwords

In het algemeen gelden de paraplumaatregelen, die onder meer betrekking dienen te hebben op bestands- en programmatuurbeveiliging. De beoordeling van deze maatregelen is ook in dit verband van belang voor het geheim houden van passwords. De bestanden, waarop de passwords zijn opgeslagen alsmede de desbetreffende software dient beveiligd te zijn tegen ongeautoriseerde toegang.

Indien een overschreden aantal pogingen tot het intoetsen van passwords wordt gelogd en vervolgens geprint, dient hiermee door de organisatie wel iets (liefst zo snel mogelijk) te worden gedaan. Dit betekent dat de accountant geïnteresseerd dient te zijn in de naleving van de procedure, die erop gericht is actie te ondernemen indien overtredingen zich voordoen.

Hoofdstuk 6. Aanvullende maatregelen

In een bezoek bij de cliënt kan de accountant vaststellen of terminals, die onbewaakt worden achtergelaten ook inderdaad zijn uitgezet (dit niet alleen uit energiebesparing).
Bij sommige software is een fysieke beveiliging van de terminal zelfs van belang. Dit betekent dat de accountant hieraan aandacht dient te schenken bij een bezoek aan de cliënt.

Hoofdstuk 7. Uitgifte passwords en beheer beveiligingsprogrammatuur

De procedure voor het verkrijgen van een gebruikersidentificatie en initieel password dient te worden beoordeeld.
De naleving dient periodiek gecontroleerd te worden. Veelal vindt in deze procedure een vastlegging/formulierenstroom plaats.
Dit zelfde geldt voor de procedure voor het herkrijgen van een vergeten password.
Voorts kan de eerdergenoemde lijst van gebruikers met passwords worden gebruikt in combinatie met overplaatsingsgegevens en informatie betreffende personeelsleden, die de organisatie hebben verlaten. Deze laatste groep dient niet meer op de meest recente lijst voor te komen. Bij de eerste groep van personeelsleden kan worden beoordeeld of voor hen nog wel toegang tot de computer noodzakelijk is. Zo niet, dan dienen ook zij evenals de ex-personeelsleden niet meer op die lijst voor te komen.

Zoals reeds genoemd in de controlemaatregelen onder hoofdstuk 5, dient de software, die password-protectie biedt, tegen ongeautoriseerde toegang te worden beschermd.

Uit het voornoemde dient duidelijk te zijn, dat:
- een en ander bijzonder afhankelijk is van de password-protectie-software;
- de accountant in dit verband een specialist dient te zijn op het gebied van voornoemde software en password-protectie.

Nochtans is het goed, dat de controlerend accountant weet of tenminste begrijpt waarom en wanneer een EDP-auditor bepaalde punten wel of niet onderzoekt, danwel dient te onderzoeken.
A. van der Drift.

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