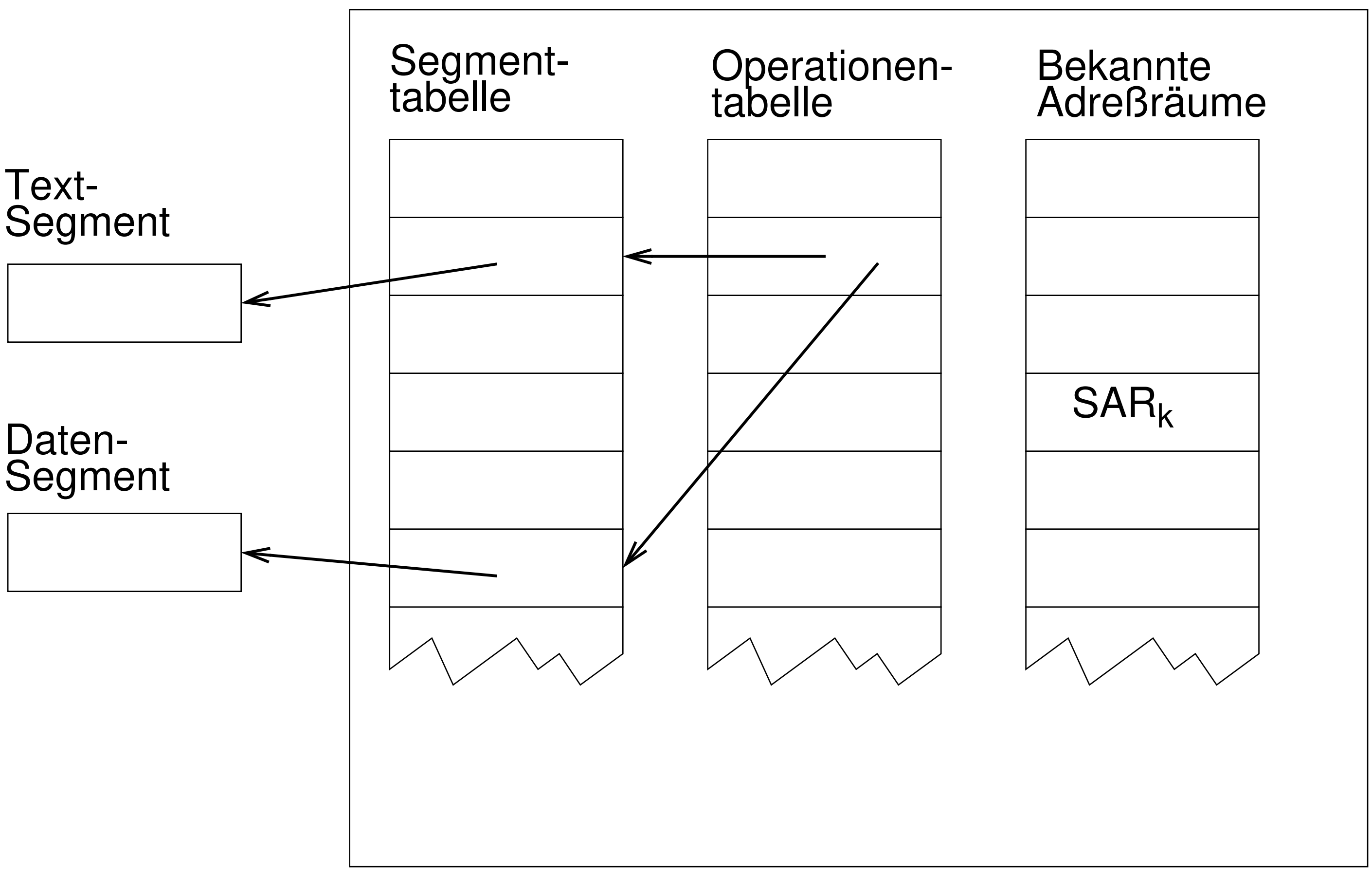
8.3 Maßnahmen auf der physikalischen Ebene

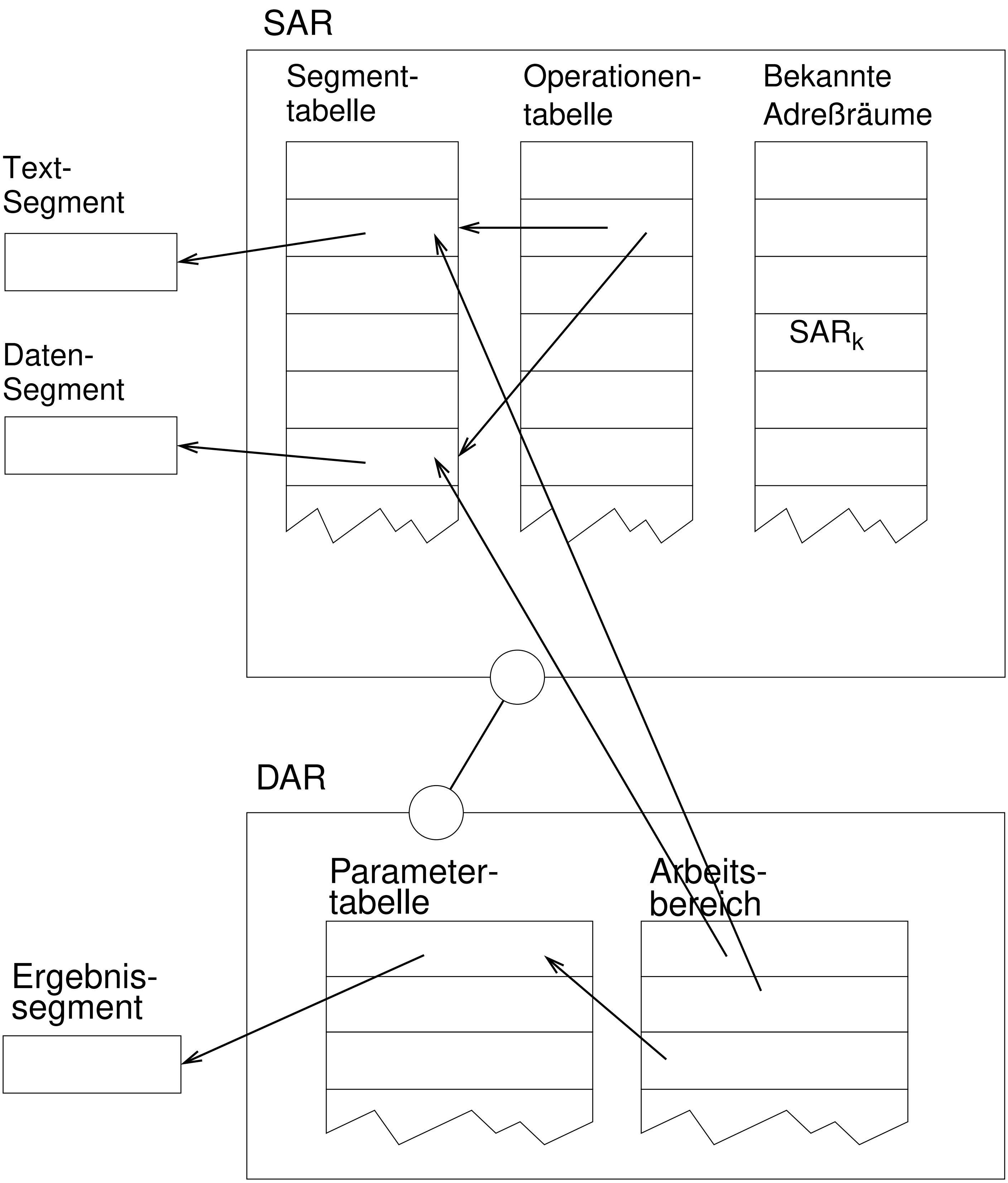
Statischer Adreßraum (SAR)



Angaben für ASCALL

1. Index eines bekannten Adreßraums
2. Index einer Operation
3. Parameterliste in Form von Indizes für Segment- und Parametertabelle
4. Index für Segment- oder Parametertabelle zur Übergabe des Ergebnissegmentes

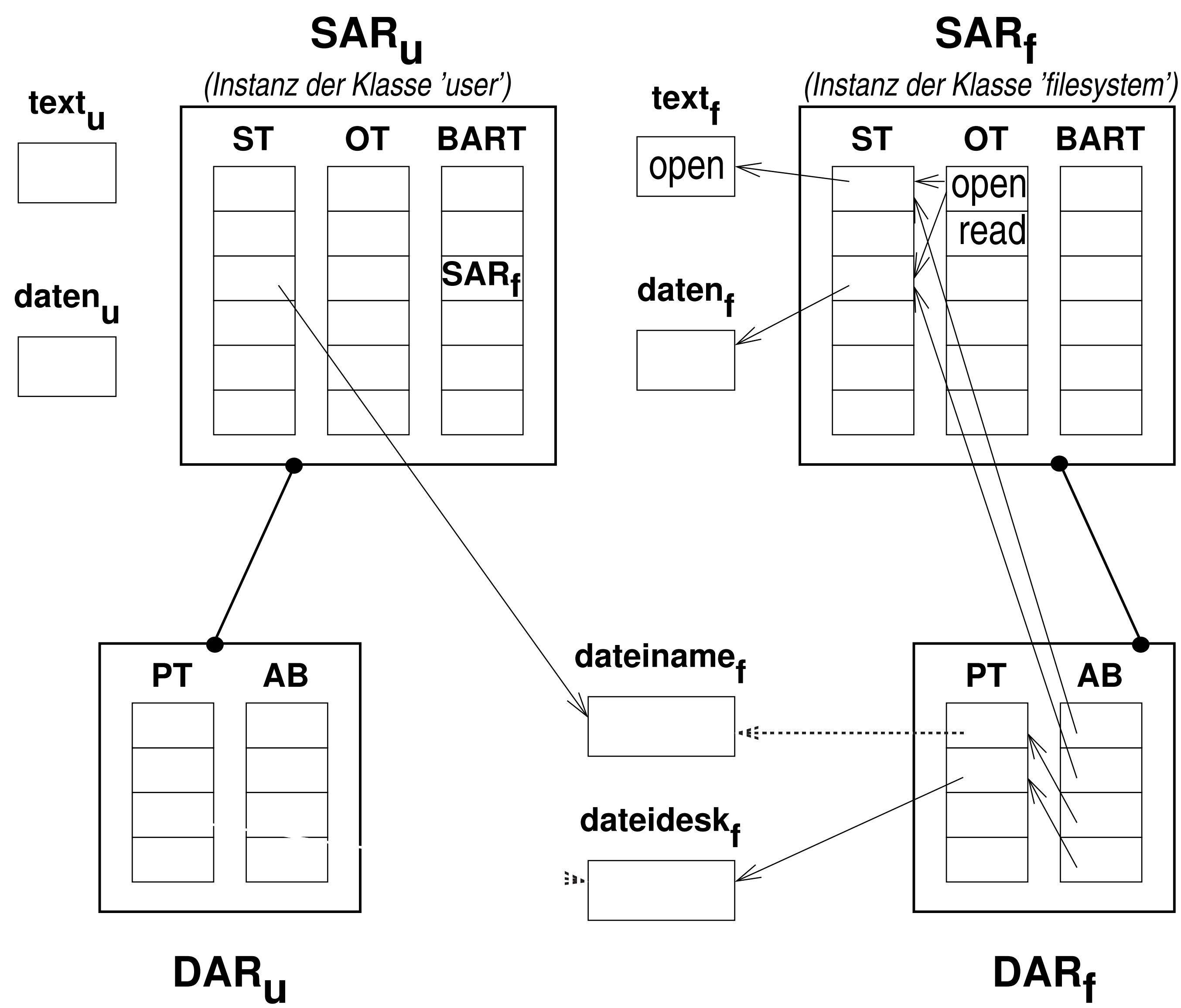
Dynamischer Adreßraum (DAR)

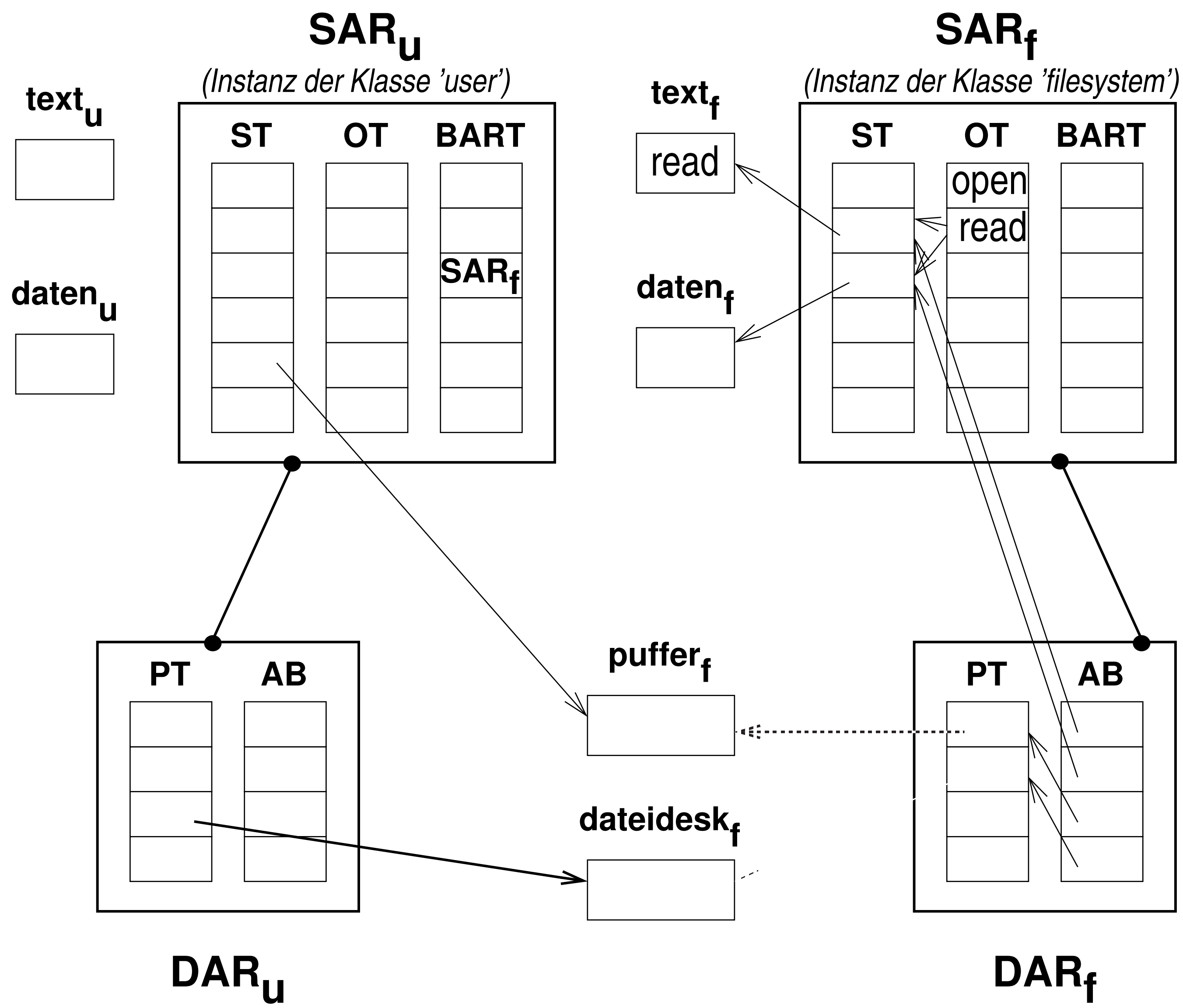


```
MODULE user(ds: &filesystem)
DECLARATIONS
   dateidesk: dateideskriptor;
   dateiname: SEQ OF CHAR;
   ...
OPERATIONS
   ...
      EFFECTS
         dateidesk=ds->open('dateiname)
   ...
```

```
MODULE filesystem;
DECLARATIONS
   ...
OPERATIONS
   ...
   open(fname)
         ->fdes: dateideskriptor
   ...
```

ASCALL(BART[3], 1, (ST[3]), PT[3])





Lesen aus einer Datei, für die ein Verweis auf den Dateideskriptor in PT[3] und ein Verweis auf einen Puffer in ST[5] steht:

ASCALL(BART[3], 2, (PT[3], ST[5]), NIL)

Grundlegende Schutzmechanismen

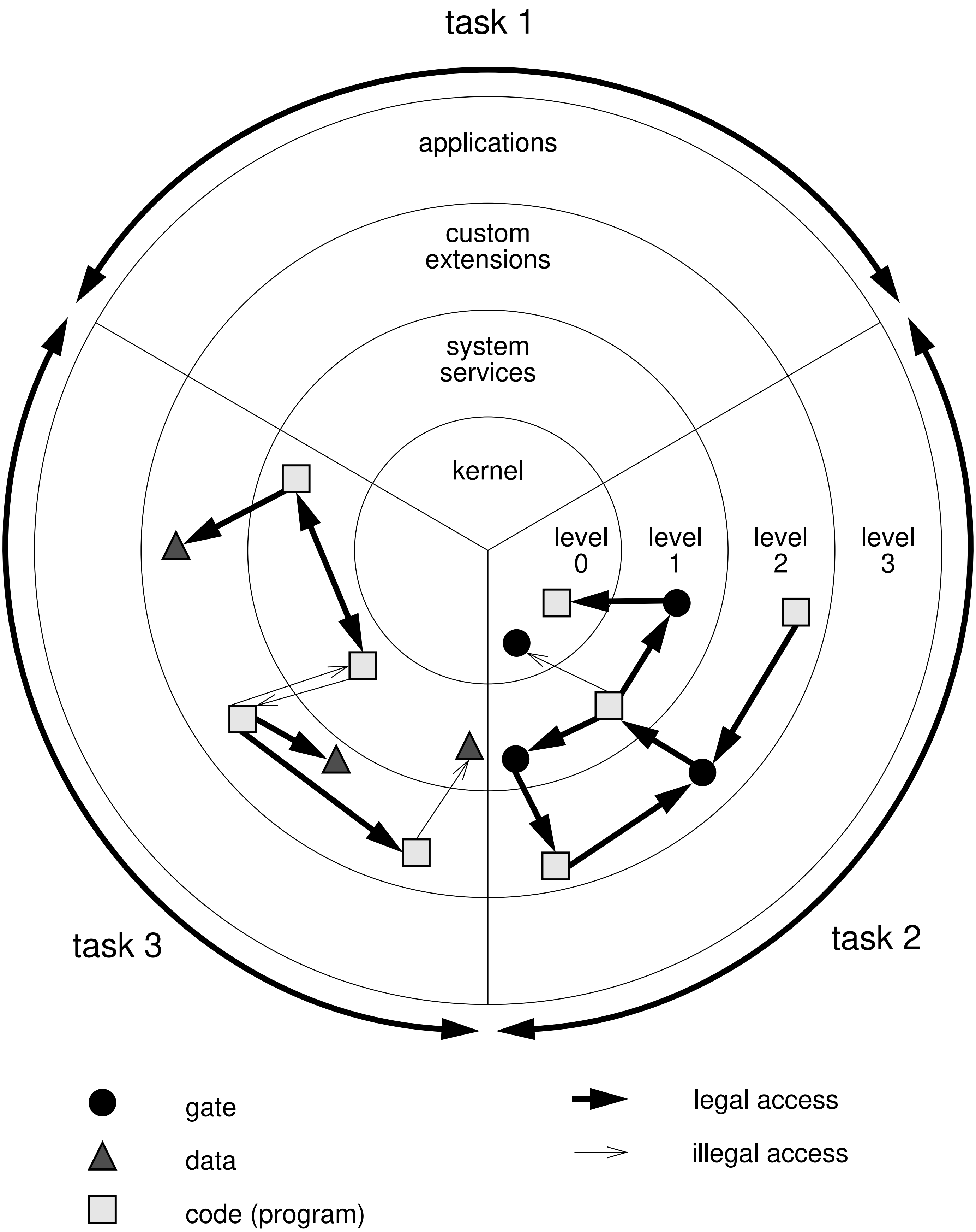
(1) Typ-Prüfung
(Datensegmente, Text(Befehls)segmente, ...)

(2) Grenzen-Prüfung
(Segmentgrenzen)

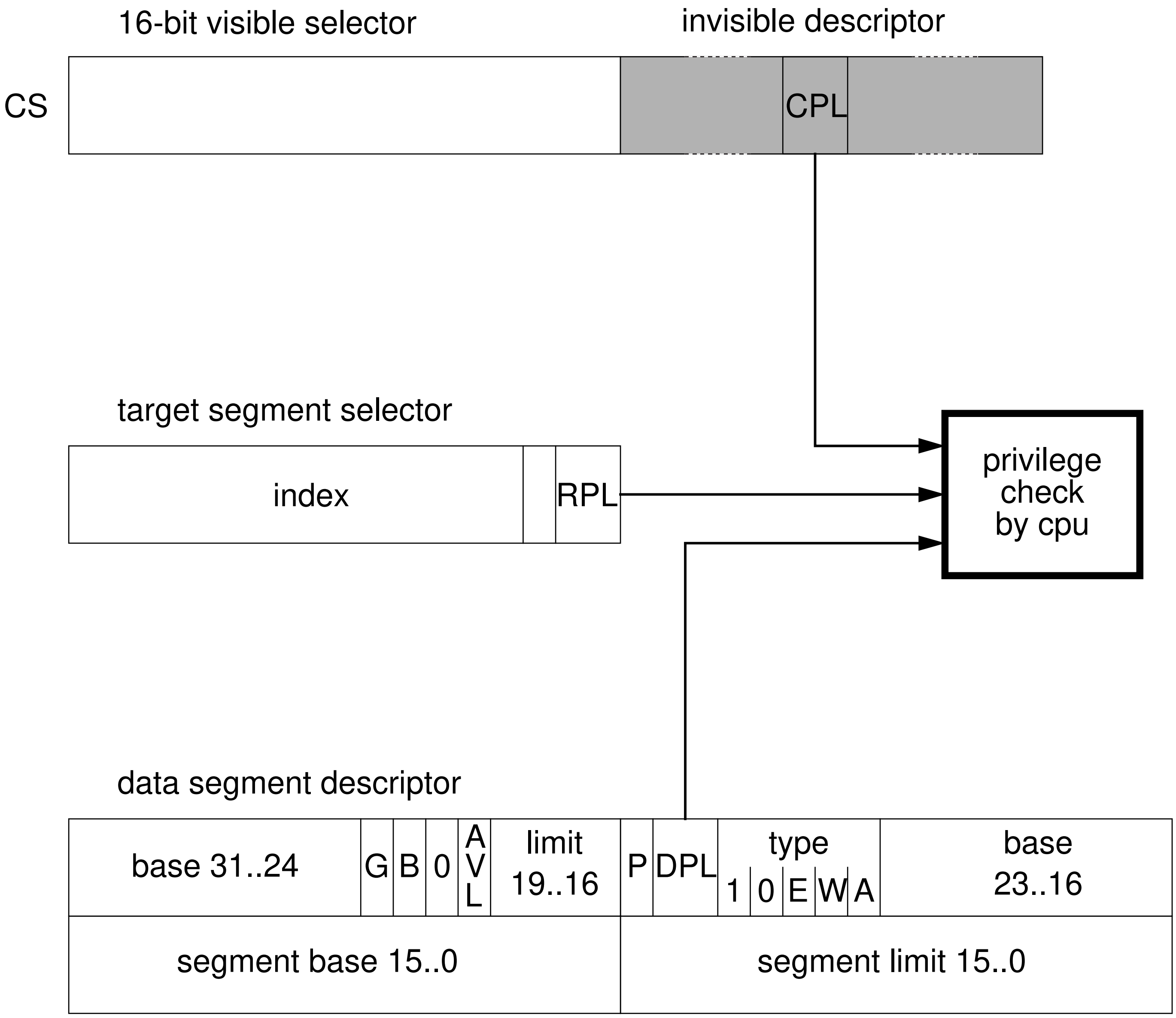
(3) Einschränkung des adressierbaren Bereichs
(prozeßspezifische Segmenttabellen)

(4) Einschränkung der Methoden-Einsprungpunkte
(Tore oder ’gates’)

(5) Einschränkung der ausführbaren Befehle
(privilegierter Befehle)


task 1
applications
custom extensions
system services
kernel
level 0
level 1
level 2
level 3
task 3
task 2
gate
data
code (program)
legal access
illegal access

Datenzugriff

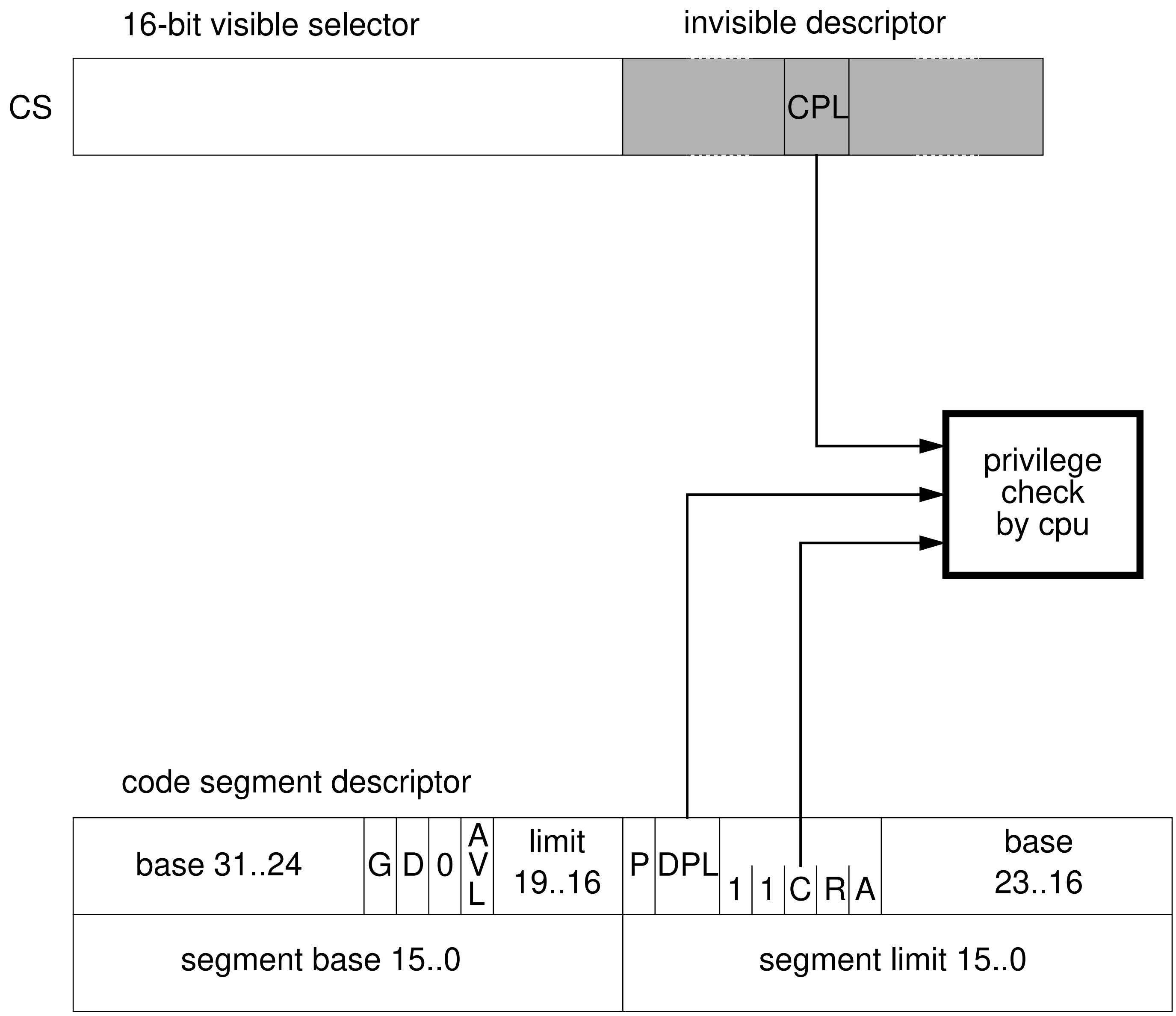


CPL - current privilege level
RPL - requestor's privilege level
DPL - descriptor privilege level

Zugangsbedingung:

$$DPL \geq \max(CPL, RPL)$$

Kontrolltransfer ohne 'gate'

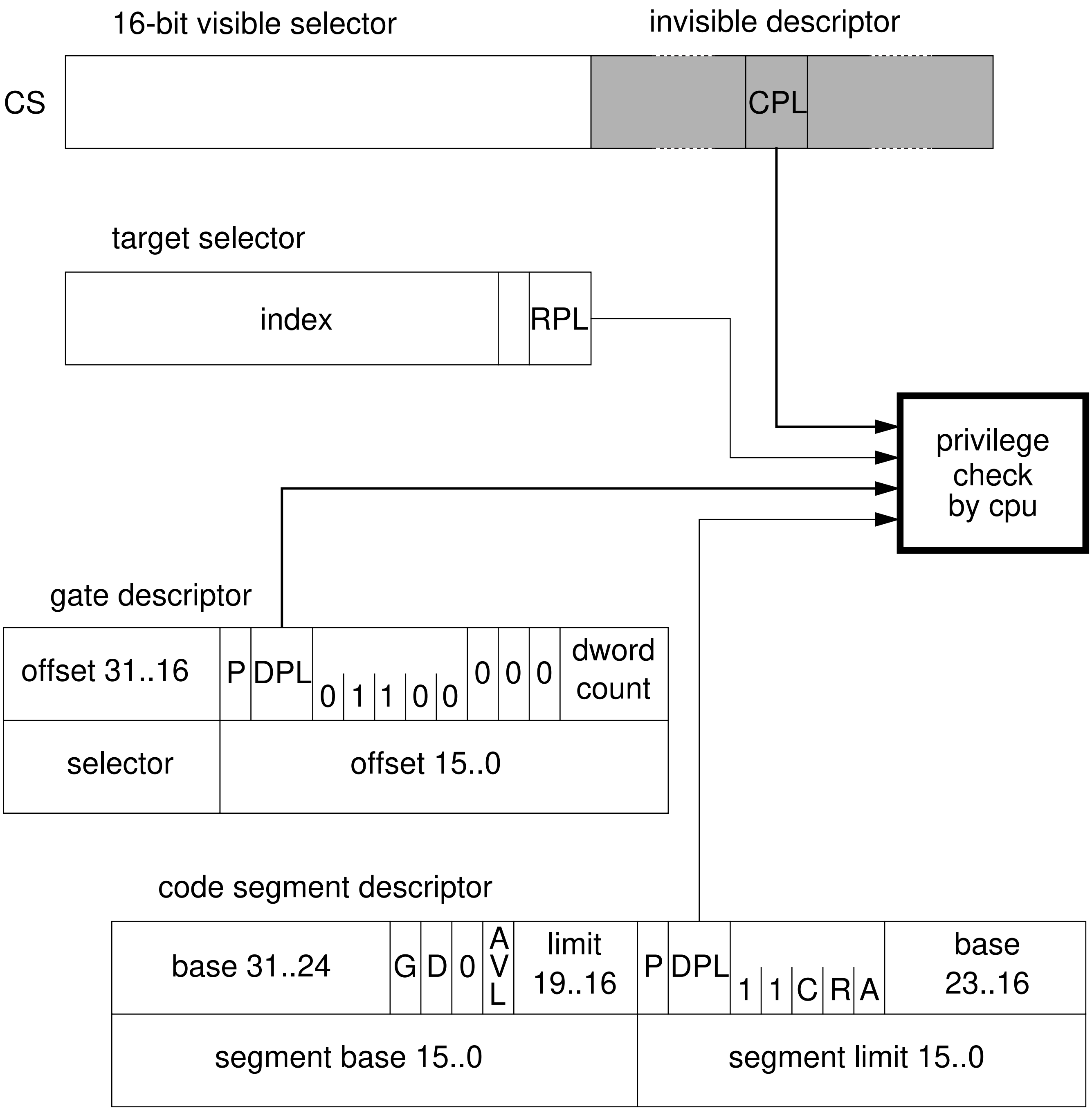


CPL - current privilege level
DPL - descriptor privilege level
C - conforming bit

Zugangsbedingung:

DPL = CPL
oder
C = 1 und DPL ≤ CPL

Kontrolltransfer mit 'gate'



Zugangsbedingung:

CPL - current privilege level
RPL - requestor's privilege level
DPL - descriptor privilege level

gate DPL $\geq$ max(CPL, RPL)

und

CPL $\geq$ target segment DPL