MACHINE m12
REFINES m11
SEES c0
VARIABLES

CA
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
CA1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
CiO1
Access_Requested
Request_Treated
time
at
PDA permission deadline assingment
Discarded_Request
height
PATH
PDistA
Final_Decision
Processing_Time
PAcA1

PAcA

INVARIANTS

inv3: $height \in UNIT \pfun \mathbb{N}$

inv4: $\forall u \cdot u \in ran(root1) \Rightarrow (height[\{u\}] \neq \varnothing \Rightarrow height(u) = 0)$

inv5: $\forall u, v \cdot u \mapsto v \in UH1 \Rightarrow (height[\{u\}] \neq \varnothing \land height[\{v\}] \neq \varnothing \Rightarrow height(u) = height(v) + 1)$

inv6: $PATH \subseteq UNIT \times UNIT$

inv7: $PDistA \subseteq PERMISSION \times \mathbb{N}$

inv8: $Final\_Decision \in Access\_Requested \pfun 0 \upto 1$

inv9: $Processing\_Time \in Access\_Requested \pfun \mathbb{N}$

inv10: $PAcA1 \in PERMISSION \pfun CiO1$

EVENTS

Initialisation ⟨extended⟩

begin

act1: $CiO := \varnothing$

act2: $root :\in ORG \pfun UNIT$

act3: $OU :\in UNIT \pfun ORG$

act4: $AiO := \varnothing$

act5: $UH :\in UNIT \pfun UNIT$

act6: $ViO := \varnothing$

act7: $RiO := \varnothing$

act9: $PCA :\in PERMISSION \pfun COR$

act10: $PRA := \varnothing$

act11: $EA := \varnothing$

act12: $UR := \varnothing$

act13: $PAA := \varnothing$

act14: $PVA := \varnothing$

act15: $PCxA := \varnothing$

act16: $AV := \varnothing$

act17: $AA := \varnothing$

act18: $RV := \varnothing$

act20: $root1 := \varnothing$

act21: $OU1 :\in UNIT \pfun ORG$

act22: $UH1 := \varnothing$

act23: $CA := \varnothing$

act24: $UR1 := \varnothing$

act25: $RiO1 := \varnothing$

act26: $EA1 := \varnothing$

act27: $CA1 := \varnothing$

act28: $PRA1 := \varnothing$

act29: $PAA1 := \varnothing$

act30: $PVA1 := \varnothing$

act31: $PCA1 := \varnothing$

act32: $PCxA1 := \varnothing$

act33: $ViO1 := \varnothing$

act34: $RV1 := \varnothing$

act35: $AiO1 := \varnothing$

act36: $AV1 := \varnothing$

act37: $AA1 := \varnothing$

act38: $CiO1 := \varnothing$

act39: $Access\_Requested := \varnothing$

act40: $PDistA := \varnothing$

act41: $Request\_Treated := \varnothing$

act42: $PAcA := \varnothing$

act43: $time := 0$

act44: $at := \varnothing$

act45: $PDA := \varnothing$

act46: $Discarded\_Request := \varnothing$

act50: $height := \varnothing$

act51: $PATH := \varnothing$
act52: $Final\_Decision := \varnothing$
act53: $Processing\_Time := \varnothing$
act54: $PAcA1 := \varnothing$

end

Event Concrete_Model_Generation ⟨ordinary⟩ $\widehat{=}$
refines Concrete_Model_Generation

begin

act1: $CiO := CiO1$
act4: $AiO := AiO1$
act6: $ViO := ViO1$
act16: $AV := AV1$
act17: $AA := AA1$
act18: $RV := RV1$
act2: $root := root1$
act5: $UH := UH1$
act3: $OU := OU1$
act7: $RiO := RiO1$
act12: $UR := UR1$
act11: $EA := EA1$
act9: $PCA := PCA1$
act10: $PRA := PRA1$
act13: $PAA := PAA1$
act14: $PVA := PVA1$
act15: $PCxA := PCxA1$
act19: $CA := CA1$
act20: $PAcA := PAcA1$

end

Event Assign_Organization_Root ⟨ordinary⟩ $\widehat{=}$
refines Assign_Oragnization_Root

any

u
org

where

grd1: $org \in ORG \land u \in UNIT$
grd2: $org \notin dom(root1)$
grd3: $u \notin dom(UH1)$
grd4: $ran(root1 \cup \{org \mapsto u\}) \cap dom(UH1) = \varnothing$
grd5: $u \mapsto org \in OU1$
grd6: $u \notin ran(root1)$
grd7: $height[\{u\}] = \varnothing$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$
act2: $height := height \lhd\!\!+ \{u \mapsto 0\}$

end

Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
refines Add_Unit_Hierarchy

any

u1
u2

where

grd1: $u1 \in UNIT \land u2 \in UNIT$
grd3: $u1 \notin dom(UH1)$
grd7: $u1 \mapsto u2 \notin UH1$
grd4: $u1 \neq u2$
grd5: $u2 \mapsto u1 \notin UH1$
grd6: $u1 \notin ran(root1)$
grd8: $OU1[\{u1\}] = OU1[\{u2\}]$

grd9: $\forall e \cdot e \mapsto u1 \in EA1 \Rightarrow e \mapsto u2 \notin EA1$
grd10: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$
grd11: $height[\{u2\}] \neq \varnothing$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$
act2: $height := height \Leftarrow \{u1 \mapsto (height(u2) + 1)\}$
act3: $PATH := PATH \cup \{u1 \mapsto u2\} \cup \{u3 \cdot u2 \mapsto u3 \in PATH | u1 \mapsto u3\}$

end

Event Assign_Unit_to_Org ⟨ordinary⟩ $\widehat{=}$
extends Assign_Unit_to_Org

any

u
org

where

grd1: $u \mapsto org \notin OU1$
grd2: $u \notin dom(OU1)$
grd3: $\forall org1, role \cdot u \mapsto (role \mapsto org1) \in UR1 \Rightarrow org = org1$

then

act1: $OU1 := OU1 \cup \{u \mapsto org\}$

end

Event Assign_Role_to_Unit ⟨ordinary⟩ $\widehat{=}$
extends Assign_Role_to_Unit

any

r
u

where

grd1: $r \in RiO1 \land u \in UNIT \land (u \mapsto r) \notin UR1$
grd2: $\forall role, org \cdot r = role \mapsto org \Rightarrow (OU1[\{u\}] \neq \varnothing \Rightarrow OU1(u) = org)$

then

act1: $UR1 := UR1 \cup \{(u \mapsto r)\}$

end

Event Assign_Role_to_Organization ⟨ordinary⟩ $\widehat{=}$
extends Assign_Role_to_Organization

any

r
org

where

grd1: $r \in ROLE \land org \in ORG$
grd2: $r \mapsto org \notin RiO1$

then

act1: $RiO1 := RiO1 \cup \{r \mapsto org\}$

end

Event Assign_Employee-to_Unit ⟨ordinary⟩ $\widehat{=}$
extends Assign_Employee-to_Unit

any

e
u

where

grd1: $e \mapsto u \notin EA1$
grd2: $\forall u1 \cdot e \mapsto u1 \in EA1 \Rightarrow (u \mapsto u1 \notin UH1 \land u1 \mapsto u \notin UH1)$

then

act1: $EA1 := EA1 \cup \{e \mapsto u\}$

end

Event Assign_Approver ⟨ordinary⟩ $\widehat{=}$
refines Assign_Approver

any

p
d

u
cor

where

grd5: $\forall u1, p1, d1 \cdot cor \mapsto u1 \mapsto p1 \mapsto d1 \in CA1 \Rightarrow u1 \neq u \wedge (u1 \mapsto u \in UH1 \vee (\exists u2, p2, d2 \cdot cor \mapsto u2 \mapsto p2 \mapsto d2 \in CA1 \wedge u2 \mapsto u \in UH1))$

grd1: $\forall u2, p2, d2 \cdot cor \mapsto u2 \mapsto p2 \mapsto d2 \in CA1 \wedge u \neq u2 \Rightarrow (OU1[\{u\}] \neq \varnothing \wedge OU1[\{u2\}] \neq \varnothing \Rightarrow OU1(u) = OU1(u2))$

grd2: $cor \mapsto u \mapsto p \mapsto d \notin CA1$

grd4: $d \in \mathbb{N} \wedge p \in \mathbb{N}$

then

act1: $CA1 := CA1 \cup \{cor \mapsto u \mapsto p \mapsto d\}$

end

Event Define_Security_Rule ⟨ordinary⟩ $\widehat{=}$

extends Define_Security_Rule

any

rio
aio
vio
cor
cio
perm

where

grd1: $rio \in RiO1 \wedge aio \in AiO \wedge vio \in ViO \wedge cio \in CiO \wedge cor \in COR \wedge perm \in PERMISSION$

grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \wedge vio = v \mapsto org2 \wedge cio = c \mapsto org3 \Rightarrow org1 = org2 \wedge org2 = org3$

grd3: $perm \notin dom(PRA1) \wedge perm \notin dom(PAA1) \wedge perm \notin dom(PVA1) \wedge perm \notin dom(PCA1) \wedge perm \notin dom(PCxA1)$

grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, p1, d1, org1 \cdot cor \mapsto u1 \mapsto p1 \mapsto d1 \in CA1 \wedge OU1(u1) = org1 \Rightarrow org1 = org)$

then

act1: $PRA1 := PRA1 \cup \{perm \mapsto rio\}$

act2: $PAA1 := PAA1 \cup \{perm \mapsto aio\}$

act3: $PVA1 := PVA1 \cup \{perm \mapsto vio\}$

act4: $PCA1 := PCA1 \cup \{perm \mapsto cor\}$

act5: $PCxA1 := PCxA1 \cup \{perm \mapsto cio\}$

act6: $PDA := PDA \cup \{perm \mapsto GLOBAL\_DEADLINE\}$

end

Event Assign_Resource_to_View ⟨ordinary⟩ $\widehat{=}$

extends Assign_Resource_to_View

any

r
vio

where

grd1: $r \in RESOURCE \wedge vio \in ViO1$

grd2: $r \mapsto vio \notin RV1$

then

act1: $RV1 := RV1 \cup \{r \mapsto vio\}$

end

Event Assign_View_to_Organization ⟨ordinary⟩ $\widehat{=}$

extends Assign_View_to_Organization

any

v
org

where

grd1: $v \in VIEW \wedge org \in ORG$

grd2: $v \mapsto org \notin ViO1$

grd3: $v \mapsto org \notin ran(RV1)$

grd4: $v \mapsto org \notin ran(AV1)$

then
act1: $ViO1 := ViO1 \cup \{v \mapsto org\}$
end
Event Assign_activity_to_Organization ⟨ordinary⟩ $\widehat{=}$
extends Assign_activity_to_Organization
any
a
org
where
grd1: $a \in ACTIVITY \land org \in ORG$
grd2: $a \mapsto org \notin AiO1$
grd3: $a \mapsto org \notin ran(AA1)$
then
act1: $AiO1 := AiO1 \cup \{a \mapsto org\}$
end
Event Assign_Action_to_Activity ⟨ordinary⟩ $\widehat{=}$
extends Assign_Action_to_Activity
any
a
aio
vio
where
grd1: $a \in ACTION \land aio \in AiO1 \land vio \in ViO1$
grd2: $a \mapsto aio \notin AA1 \land a \mapsto vio \notin AV1$
then
act1: $AA1 := AA1 \cup \{a \mapsto aio\}$
act2: $AV1 := AV1 \cup \{a \mapsto vio\}$
end
Event Assign_Context_to_Organization ⟨ordinary⟩ $\widehat{=}$
extends Assign_Context_to_Organization
any
org
c
where
grd1: $org \in ORG \land c \in CONTEXT$
grd2: $c \mapsto org \notin CiO1$
then
act1: $CiO1 := CiO1 \cup \{c \mapsto org\}$
end
Event Request_Access ⟨ordinary⟩ $\widehat{=}$
refines Request_Access
any
e
a
o
t
dist
ac
d
where
grd1: $e \in EMPLOYEE \land a \in ACTION \land o \in RESOURCE \land t \in \mathbb{N}_1$
grd3: $dist \in ran(PDistA)$
grd8: $ac \in CONTEXT$
grd6: $d \in \mathbb{N}$
grd4: $\forall e1, a1, o1, t1, dl, d1, ctx \cdot t1 \mapsto e1 \mapsto a1 \mapsto o1 \mapsto dl \mapsto d1 \mapsto ctx \in Access\_Requested \Rightarrow t > t1$
grd2: $\exists u, r, v, p, org, act, c, rio, aio, vio, cio, acio \cdot e \mapsto u \in EA \land u \mapsto org \in OU \land rio = (r \mapsto org) \land rio \in RiO \land u \mapsto rio \in UR \land p \mapsto rio \in PRA \land vio = (v \mapsto org) \land vio \in ViO \land o \mapsto vio \in RV \land (p \mapsto vio) \in PVA \land aio = (act \mapsto org) \land (p \mapsto aio) \in PAA \land a \mapsto vio \in AV \land (a \mapsto aio) \in AA \land cio = (c \mapsto org) \land (p \mapsto cio) \in PCxA \land (p \mapsto dist) \in PDistA \land acio = (ac \mapsto org) \land (p \mapsto acio) \in PAcA \land (p \mapsto d) \in PDA$

grd7: $dist \in ran(PDistA)$
grd5: $t > time$

then

act1: $Access\_Requested := Access\_Requested \cup \{t \mapsto e \mapsto a \mapsto o \mapsto d \mapsto dist \mapsto ac\}$
act2: $at := at \cup \{t\}$

end

Event Treat_Request ⟨ordinary⟩ $\widehat{=}$

refines Treat_Request

any

r
s
t
dec

where

grd1: $r \in Access\_Requested \land t \in \mathbb{N}_1$
grd8: $dec \in 0 \mathinner{..} 1$
grd3: $\forall t1, s1, dec1 \cdot t1 \mapsto r \mapsto s1 \mapsto dec1 \in Request\_Treated \Rightarrow t > t1 \land s1 \neq s$
approve once per approver
grd4: $\forall u, u1, t1, s1, dec1 \cdot s \mapsto u \in EA \land s1 \mapsto u1 \in EA \land t1 < t \land t1 \mapsto r \mapsto s1 \mapsto dec1 \in Request\_Treated \Rightarrow u \neq u1$
approve once per unit
grd5: $\forall e, a, o, t0, dist, d, ac \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto d \mapsto dist \mapsto ac \Rightarrow EA(s) \in PATH[\{EA(e)\}]$
grd6: $\forall e, a, o, t0, dist, d, ac \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto d \mapsto dist \mapsto ac \Rightarrow height(EA(e)) - height(EA(s)) \leq dist$
grd7: $\forall e, a, o, t0, dist, d, ac, current \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto d \mapsto dist \mapsto ac \land current = card(\{tr, t1, s1, dec1 \cdot tr = t1 \mapsto r \mapsto s1 \mapsto dec1 \land tr \in Request\_Treated | tr\}) \Rightarrow t \leq max(\{t0\} \cup \{t1, s1, dec1 \cdot t1 \mapsto r \mapsto s1 \mapsto dec1 \in Request\_Treated | t1\}) + (height(EA(e)) - height(EA(s)) - current) * d$
grd9: $\forall e, a, o, t0, dist, d, ac \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto d \mapsto dist \mapsto ac \Rightarrow isTrue(ac) = TRUE$

then

act1: $Request\_Treated := Request\_Treated \cup \{t \mapsto r \mapsto s \mapsto dec\}$
act2 : $at := at \setminus \{time\}$

end

Event Execute_Request ⟨ordinary⟩ $\widehat{=}$

any

r
t

where

grd1: $r \in Access\_Requested$
grd2: $r \notin dom(Final\_Decision)$
grd4: $t \in \mathbb{N}$
grd3: $\forall e, a, o, t0, dist, d, total, last, ac \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto d \mapsto dist \mapsto ac \land total = card(\{tr, t1, s1, dec \cdot tr = t1 \mapsto r \mapsto s1 \mapsto dec \land tr \in Request\_Treated | tr\}) \land last = max(\{t0\} \cup \{t1, s1, dec \cdot t1 \mapsto r \mapsto s1 \mapsto dec \in Request\_Treated | t1\}) \Rightarrow (dist = total \land t = last) \lor (t = last + (dist - total) * d \land time \geq t)$

then

act1: $Final\_Decision(r) := max(\{0\} \cup \{last, s, dec \cdot last = max(\{t1, s1, dec1 \cdot t1 \mapsto r \mapsto s1 \mapsto dec1 \in Request\_Treated | t1\}) \land last \mapsto r \mapsto s \mapsto dec \in Request\_Treated | dec\})$
act2: $Processing\_Time(r) := t$

end

Event tick_tock ⟨ordinary⟩ $\widehat{=}$

extends tick_tock

any

tm

where

grd1: $tm \in \mathbb{N} \land tm > time \land (at \neq \varnothing \Rightarrow tm \leq min(at))$

then

act1: $time := tm$

end

Event Assign_Approval_Deadline ⟨ordinary⟩ $\widehat{=}$
refines Assign_Approval_Deadline
any
p
d
where
grd1: $p \in PERMISSION \land d \in \mathbb{N}$
grd2: $p \mapsto d \notin PDA$
then
act1: $PDA := PDA \lhd\!\!\!- \{p \mapsto d\}$
end
Event Assign_approval_perimeter ⟨ordinary⟩ $\widehat{=}$
any
dist
perm
where
grd1: $perm \mapsto dist \notin PDistA$
then
act1: $PDistA := PDistA \cup \{perm \mapsto dist\}$
end
Event Assign_Approval_Context ⟨ordinary⟩ $\widehat{=}$
any
c
p
where
grd1: $p \mapsto c \notin PAcA1$
grd2: $c \in CiO1$
then
act1: $PAcA1 := PAcA1 \cup \{p \mapsto c\}$
end
END