Contents

CONTEXT c0

SETS

UNIT
ORG
ROLE
EMPLOYEE
CONTEXT
VIEW
ACTIVITY
RESOURCE
ACTION
PERMISSION
COR

CONSTANTS

GLOBAL_DEADLINE

AXIOMS

axm1: $finite(UNIT) \land finite(ORG) \land finite(ROLE) \land finite(EMPLOYEE) \land finite(CONTEXT)$

axm2: $finite(PERMISSION)$

axm3: $finite(ACTIVITY) \land finite(ACTION) \land finite(VIEW) \land finite(RESOURCE)$

axm4: $finite(COR)$

axm5: $GLOBAL\_DEADLINE \in \mathbb{N}$

END

MACHINE m0

This machine defines the abstarct machine and generates an abstract model which will be refine further

SEES c0

VARIABLES

UH
PCA
root
OU
RiO
PRA
EA
UR
ViO
AiO
PAA
PVA
CiO
PCxA
RV
AV
AA
Approver

INVARIANTS

inv1: $CiO \subseteq CONTEXT \times ORG$
context in organization

inv2: $root \in ORG \nrightarrow UNIT$
root of the organization

inv3: $OU \in UNIT \nrightarrow ORG$
unit to organization mapping

inv4: $AiO \subseteq ACTIVITY \times ORG$
activity to organization mapping

inv5: $UH \in UNIT \nrightarrow UNIT$
unit hierarchy: many to one unit to unit relationship

inv6: $ViO \subseteq VIEW \times ORG$
view to org mapping

inv7: $RiO \subseteq ROLE \times ORG$
role to org mapping

inv8: $Approver \subseteq COR \times OU$
chain of command approver mapping

inv9: $PCA \in PERMISSION \nrightarrow COR$
permission to chain of command mapping

inv10: $PRA \in PERMISSION \nrightarrow RiO$
permission to role assigment

inv11: $EA \subseteq EMPLOYEE \times UNIT$
many to many employee to unit assingment

inv12: $UR \subseteq UNIT \times RiO$
unit to role assingment

inv13: $PAA \in PERMISSION \nrightarrow AiO$
permission to activity mapping

inv14: $PVA \in PERMISSION \nrightarrow ViO$
permission to view mapping

inv15: $PCxA \in PERMISSION \nrightarrow CiO$
permission to context mapping

inv16: $AV \subseteq ACTION \times ViO$
action to view mapping
inv17: $AA \subseteq ACTION \times AiO$
action to activity mapping
inv18: $RV \subseteq RESOURCE \times ViO$
resource to view mapping

EVENTS

Initialisation

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: $RV := \varnothing$
act19: $Approver := \varnothing$

end

Event Abstract_Model_Generation ⟨ordinary⟩ $\widehat{=}$
This event generates an abstract model without constraints chsking. It will be further refined to more concrete one.

any

rio
aio
vio
cio
uh
ea
ou
rt
ur
aa
av
rv
approver
pra
paa
pva
pca
pcxa

where

grd2: $rio \subseteq ROLE \times ORG$
grd4: $aio \in \mathbb{P}(ACTIVITY \times ORG)$
grd5: $vio \subseteq VIEW \times ORG$
grd6: $cio \subseteq CONTEXT \times ORG$
grd7: $uh \in UNIT \pfun UNIT$
grd8: $ea \subseteq EMPLOYEE \times UNIT$
grd9: $ou \in UNIT \pfun ORG$
grd10: $cio \subseteq CONTEXT \times ORG$

grd11: $rt \in ORG \pfun UNIT$
grd12: $ur \subseteq UNIT \times rio$
grd13: $av \subseteq ACTION \times vio$
grd14: $aa \subseteq ACTION \times aio$
grd15: $rv \subseteq RESOURCE \times vio$
grd16: $approver \subseteq COR \times ou$
grd17: $pra \in PERMISSION \pfun rio$
grd18: $paa \in PERMISSION \pfun aio$
grd19: $pva \in PERMISSION \pfun vio$
grd20: $pcxa \in PERMISSION \pfun cio$
grd21: $pca \in PERMISSION \pfun COR$

then

act1: $CiO := cio$
act2: $root := rt$
act3: $OU := ou$
act4: $AiO := aio$
act5: $UH := uh$
act6: $ViO := vio$
act7: $RiO := rio$
act8: $Approver := approver$
act9: $PCA := pca$
act10: $PRA := pra$
act11: $EA := ea$
act12: $UR := ur$
act13: $PAA := paa$
act14: $PVA := pva$
act15: $PCxA := pcxa$
act16: $AV := av$
act17: $AA := aa$
act18: $RV := rv$

end

END

MACHINE m1

This event defines organization hierarchy: root, unit to organization assigment and unit hierarahy

REFINES m0

SEES c0

VARIABLES

PCA
root
OU
RiO
UH
PRA
EA
UR
ViO
AiO
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
Approver

INVARIANTS

inv2: $UH1 \in UNIT \pfun UNIT$
The variable UH1 is a concrete variable of UH

inv3: $UH1 \cap id = \varnothing$
unit hierarchy is not refllexive eg. u $\mapsto$ u $\notin$ UH1

inv4: $UH1 \cap UH1^{-1} = \varnothing$
hierarchy is asymmetric

inv5: ⟨theorem⟩ $\forall u1, u2, u3 \cdot (u1 \mapsto u2) \in UH1 \land (u1 \mapsto u3) \in UH1 \Rightarrow u2 = u3$
the hierarchy of a node is unique

inv7: $OU1 \in UNIT \pfun ORG$
a unit is mapped to only one organization

inv1: $root1 \in ORG \pfun dom(OU1)$
an organization root is mapped to only one unit

inv10: $\forall org1, org2, u \cdot (org1 \mapsto u) \in root1 \land (org2 \mapsto u) \in root1 \Rightarrow org1 = org2$
uniqueness of root unit

inv6: $ran(root1) \cap dom(UH1) = \varnothing$
a root unit is not subordinated

inv8: $\forall u, org \cdot org \mapsto u \in root1 \Rightarrow u \mapsto org \in OU1$
root should belong to the organization

inv9: $\forall us, um \cdot us \mapsto um \in UH1 \Rightarrow (OU1[\{us\}] \neq \varnothing \land OU1[\{um\}] \neq \varnothing \Rightarrow OU1(us) = OU1(um))$
the hierarchy belongs to an organization

EVENTS

Initialisation

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: $Approver := \varnothing$

end

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

any

rio
aio
vio
cio
ea
ou
ur
aa
av
rv
approver
pra
paa
pva
pca
pcxa

where

grd2: $rio \subseteq ROLE \times ORG$
grd4: $aio \in \mathbb{P}(ACTIVITY \times ORG)$
grd5: $vio \subseteq VIEW \times ORG$
grd6: $cio \subseteq CONTEXT \times ORG$
grd8: $ea \subseteq EMPLOYEE \times UNIT$
grd9: $ou \in UNIT \pfun ORG$
grd10: $cio \subseteq CONTEXT \times ORG$
grd12: $ur \subseteq UNIT \times rio$
grd13: $av \subseteq ACTION \times vio$
grd14: $aa \subseteq ACTION \times aio$
grd15: $rv \subseteq RESOURCE \times vio$
grd16: $approver \subseteq COR \times ou$
grd17: $pra \in PERMISSION \pfun rio$
grd18: $paa \in PERMISSION \pfun aio$
grd19: $pva \in PERMISSION \pfun vio$
grd20: $pcxa \in PERMISSION \pfun cio$
grd21: $pca \in PERMISSION \pfun COR$

with

rt: $rt = root1$
uh: $uh = UH1$

then

act1: $CiO := cio$
act3: $OU := ou$
act4: $AiO := aio$
act6: $ViO := vio$
act7: $RiO := rio$
act9: $PCA := pca$
act10: $PRA := pra$
act11: $EA := ea$
act12: $UR := ur$
act13: $PAA := paa$
act14: $PVA := pva$
act15: $PCxA := pcxa$
act16: $AV := av$
act17: $AA := aa$
act18: $RV := rv$
act2: $root := root1$
act5: $UH := UH1$
act8: $Approver := approver$

end

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

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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

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

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: $u1 \in dom(OU1) \land u2 \in dom(OU1)$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

end

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

any

u
org

where

grd1: $u \mapsto org \notin OU1$
grd2: $u \notin dom(OU1)$
grd3: $u \in dom(UH1) \Rightarrow (OU1[\{UH1(u)\}] \neq \varnothing \Rightarrow OU1(UH1(u)) = org)$
grd4: $u \in ran(UH1) \Rightarrow (\forall u1 \cdot u1 \mapsto u \in UH1 \Rightarrow (OU1[\{u1\}] \neq \varnothing \Rightarrow OU1(u1) = org))$

then

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

end

END

MACHINE m2

Assign Role to organization and unit to role

REFINES m1

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1

INVARIANTS

inv1: $RiO1 \subseteq ROLE \times ORG$

inv2: $UR1 \subseteq UNIT \times RiO1$

inv3: $\forall u, org, role \cdot u \mapsto (role \mapsto org) \in UR1 \Rightarrow (OU1[\{u\}] \neq \varnothing \Rightarrow OU1(u) = org)$

organization conservation

EVENTS

Initialisation ⟨extended⟩

begin

act1: $CiO := \varnothing$
act2: $root :\in ORG \nrightarrow UNIT$
act3: $OU :\in UNIT \nrightarrow ORG$
act4: $AiO := \varnothing$
act5: $UH :\in UNIT \nrightarrow UNIT$
act6: $ViO := \varnothing$
act7: $RiO := \varnothing$
act9: $PCA :\in PERMISSION \nrightarrow COR$
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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$

end

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

refines Abstract_Model_Generation

any

aio
vio
cio
ea
aa
av
rv
approver
pra
paa
pva
pca
pcxa

where

grd4: $aio \in \mathbb{P}(ACTIVITY \times ORG)$
grd5: $vio \subseteq VIEW \times ORG$
grd6: $cio \subseteq CONTEXT \times ORG$
grd8: $ea \subseteq EMPLOYEE \times UNIT$
grd10: $cio \subseteq CONTEXT \times ORG$
grd13: $av \subseteq ACTION \times vio$
grd14: $aa \subseteq ACTION \times aio$
grd15: $rv \subseteq RESOURCE \times vio$
grd17: $pra \in PERMISSION \pfun RiO1$
grd18: $paa \in PERMISSION \pfun aio$
grd19: $pva \in PERMISSION \pfun vio$
grd20: $pcxa \in PERMISSION \pfun cio$
grd21: $pca \in PERMISSION \pfun COR$
grd16: $approver \subseteq COR \times OU1$

with

ur: $ur = UR1$
rio: $rio = RiO1$ parameter susbtitution using witness
ou: $ou = OU1$

then

act1: $CiO := cio$
act4: $AiO := aio$
act6: $ViO := vio$
act9: $PCA := pca$
act10: $PRA := pra$
act11: $EA := ea$
act13: $PAA := paa$
act14: $PVA := pva$
act15: $PCxA := pcxa$
act16: $AV := av$
act17: $AA := aa$
act18: $RV := rv$
act2: $root := root1$
act5: $UH := UH1$
act8: $Approver := approver$
act3: $OU := OU1$
act7: $RiO := RiO1$

act12: $UR := UR1$

end

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

extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

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

extends 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: $u1 \in dom(OU1) \land u2 \in dom(OU1)$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

end

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

refines 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⟩ $\widehat{=}$

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⟩ $\widehat{=}$

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

END

MACHINE m3

Assign employee to unit

REFINES m2

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1

INVARIANTS

inv1: $EA1 \subseteq EMPLOYEE \times UNIT$

inv2: $\forall u1, u2, e \cdot u1 \mapsto u2 \in UH1 \land e \mapsto u1 \in EA1 \Rightarrow e \mapsto u2 \notin EA1$

Employee cannot be his own supervisor

EVENTS

Initialisation

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$

end

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

any

aio
vio
cio
aa
av
rv
pra
paa
pva
pca
pcxa
approver

where

grd4: $aio \in \mathbb{P}(ACTIVITY \times ORG)$
grd5: $vio \subseteq VIEW \times ORG$
grd6: $cio \subseteq CONTEXT \times ORG$
grd13: $av \subseteq ACTION \times vio$
grd14: $aa \subseteq ACTION \times aio$
grd15: $rv \subseteq RESOURCE \times vio$
grd17: $pra \in PERMISSION \pfun RiO1$
grd18: $paa \in PERMISSION \pfun aio$
grd19: $pva \in PERMISSION \pfun vio$
grd20: $pcxa \in PERMISSION \pfun cio$
grd21: $pca \in PERMISSION \pfun COR$
grd16: $approver \subseteq COR \times OU1$

with

ea: $ea = EA1$

then

act1: $CiO := cio$
act4: $AiO := aio$
act6: $ViO := vio$
act9: $PCA := pca$
act10: $PRA := pra$
act13: $PAA := paa$
act14: $PVA := pva$
act15: $PCxA := pcxa$
act16: $AV := av$
act17: $AA := aa$
act18: $RV := rv$
act2: $root := root1$
act5: $UH := UH1$
act8: $Approver := approver$
act3: $OU := OU1$
act7: $RiO := RiO1$
act12: $UR := UR1$
act11: $EA := EA1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$
then
act1: $root1 := root1 \cup \{org \mapsto u\}$
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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$
then
act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$
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⟩ $\widehat{=}$

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

END

MACHINE m4

Define chain of command and create security rules

REFINES m3

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1

INVARIANTS

inv1: $Approver1 \subseteq COR \times OU1$
inv3: $PRA1 \in PERMISSION \pfun RiO1$
inv4: $PAA1 \in PERMISSION \pfun AiO$
inv5: $PVA1 \in PERMISSION \pfun ViO$
inv6: $PCA1 \in PERMISSION \pfun COR$
inv7: $PCxA1 \in PERMISSION \pfun CiO$
inv2: $\forall cor, org \cdot org \in ran(Approver1[\{cor\}]) \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver1[\{cor\}] \Rightarrow org1 = org)$

organization conservation

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: $PCA :\in PERMISSION \nrightarrow COR$
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: $OU1 :\in UNIT \nrightarrow ORG$
act22: $UH1 := \varnothing$
act23: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
act28: $PRA1 := \varnothing$
act29: $PAA1 := \varnothing$
act30: $PVA1 := \varnothing$
act31: $PCA1 := \varnothing$
act32: $PCxA1 := \varnothing$

end

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

any

aio
vio
cio
aa
av
rv

where

grd4: $aio \in \mathbb{P}(ACTIVITY \times ORG)$
grd5: $vio \subseteq VIEW \times ORG$
grd6: $cio \subseteq CONTEXT \times ORG$
grd13: $av \subseteq ACTION \times vio$
grd14: $aa \subseteq ACTION \times aio$
grd15: $rv \subseteq RESOURCE \times vio$

with

approver: $approver = Approver1$
pra: $pra = PRA1$
paa: $paa = PAA1$
pva: $pva = PVA1$
pca: $pca = PCA1$
pcxa: $pcxa = PCxA1$

then

act1: $CiO := cio$
act4: $AiO := aio$
act6: $ViO := vio$
act16: $AV := av$
act17: $AA := aa$
act18: $RV := rv$
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: $Approver := Approver1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$
then
act1: $root1 := root1 \cup \{org \mapsto u\}$
end

Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$
then
act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$
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⟩ $\widehat{=}$

any

ou
cor

where

grd1: $ou \in OU1 \land cor \in COR$
grd2: $cor \mapsto ou \notin Approver1$
grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

end

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

any

rio
aio
vio
cor
cio
perm

where

grd1: $rio \in RiO1 \land aio \in AiO \land vio \in ViO \land cio \in CiO \land cor \in COR \land perm \in PERMISSION$
grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \land vio = v \mapsto org2 \land cio = c \mapsto org3 \Rightarrow org1 = org2 \land org2 = org3$
grd3: $perm \notin dom(PRA1) \land perm \notin dom(PAA1) \land perm \notin dom(PVA1) \land perm \notin dom(PCA1) \land perm \notin dom(PCxA1)$
grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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

end

END

MACHINE m5

Assign view to organization and resource to view, variables ViO1 & RV1 are concretes one

REFINES m4

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1

INVARIANTS

inv1: $ViO1 \subseteq VIEW \times ORG$

inv2: $RV1 \subseteq RESOURCE \times ViO1$

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
act28: $PRA1 := \varnothing$
act29: $PAA1 := \varnothing$
act30: $PVA1 := \varnothing$
act31: $PCA1 := \varnothing$
act32: $PCxA1 := \varnothing$
act33: $ViO1 := \varnothing$
act34: $RV1 := \varnothing$

end

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

refines Abstract_Model_Generation

any

aio
cio
aa
av

where

grd4: $aio \in \mathbb{P}(ACTIVITY \times ORG)$
grd10: $cio \subseteq CONTEXT \times ORG$
grd13: $av \subseteq ACTION \times ViO1$
grd14: $aa \subseteq ACTION \times aio$

with

rv: $rv = RV1$
vio: $vio = ViO1$

then

act1: $CiO := cio$
act4: $AiO := aio$
act6: $ViO := ViO1$
act16: $AV := av$
act17: $AA := aa$
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: $Approver := Approver1$

end

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

extends 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: $u \notin ran(root1)$
then
act1: $root1 := root1 \cup \{org \mapsto u\}$
end
Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$
then
act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$
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⟩ $\widehat{=}$
extends Assign_Approver

any

ou
cor

where

grd1: $ou \in OU1 \land cor \in COR$
grd2: $cor \mapsto ou \notin Approver1$
grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

end

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

any

rio
aio
vio
cor
cio
$perm$

where

grd1: $rio \in RiO1 \land aio \in AiO \land vio \in ViO \land cio \in CiO \land cor \in COR \land perm \in PERMISSION$
grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \land vio = v \mapsto org2 \land cio = c \mapsto org3 \Rightarrow org1 = org2 \land org2 = org3$
grd3: $perm \notin dom(PRA1) \land perm \notin dom(PAA1) \land perm \notin dom(PVA1) \land perm \notin dom(PCA1) \land perm \notin dom(PCxA1)$
grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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

end

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

any

r
vio

where

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

grd2: $r \mapsto vio \notin RV1$

then

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

end

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

any

v

org

where

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

grd2: $v \mapsto org \notin ViO1$

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

then

act1: $ViO1 := ViO1 \cup \{v \mapsto org\}$

end

END

MACHINE m6

Assign action to activity and view

REFINES m5

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1

INVARIANTS

inv1: $AiO1 \subseteq ACTIVITY \times ORG$
inv2: $AV1 \subseteq ACTION \times ViO1$
inv3: $AA1 \subseteq ACTION \times AiO1$

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $AA1 := \varnothing$

end

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

any
cio
where
grd10: $cio \subseteq CONTEXT \times ORG$
with
aio: $aio = AiO1$
aa: $aa = AA1$
av: $av = AV1$
then
act1: $CiO := cio$
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: $Approver := Approver1$

end

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

extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

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

extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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⟩ $\widehat{=}$

extends Assign_Approver

any

ou

cor

where

grd1: $ou \in OU1 \land cor \in COR$

grd2: $cor \mapsto ou \notin Approver1$

grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

end

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

extends Define_Security_Rule

any

rio

aio

vio

cor

cio

$perm$

where

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

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

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

grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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

end

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

extends Assign_Resource_to_View

any
r
vio
where
grd1: $r \in RESOURCE \land vio \in ViO1$
grd2: $r \mapsto vio \notin RV1$
then
act1: $RV1 := RV1 \cup \{r \mapsto vio\}$
end

Event Assign_View_to_Organization ⟨ordinary⟩ $\widehat{=}$
refines Assign_View_to_Organization
any
v
org
where
grd1: $v \in VIEW \land org \in ORG$
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⟩ $\widehat{=}$
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⟩ $\widehat{=}$
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

END

MACHINE m7

Assign context to organization

REFINES m6

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
CiO1

INVARIANTS

inv1: $CiO1 \subseteq CONTEXT \times ORG$

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $CiO1 := \varnothing$

end

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

with

cio: $cio = CiO1$

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: $Approver := Approver1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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

then

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

end

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

extends Assign_Approver

any

ou

cor

where

grd1: $ou \in OU1 \wedge cor \in COR$

grd2: $cor \mapsto ou \notin Approver1$

grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

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: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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

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: $v \in VIEW \land org \in ORG$
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⟩ $\widehat{=}$
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
END

MACHINE m8

Simple permission check without action

REFINES m7

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $CiO1 := \varnothing$

end

Event Concrete_Model_Generation ⟨ordinary⟩ $\widehat{=}$
extends 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: $Approver := Approver1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

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

extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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⟩ $\widehat{=}$
extends Assign_Approver
any
ou
cor
where
grd1: $ou \in OU1 \land cor \in COR$
grd2: $cor \mapsto ou \notin Approver1$
grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$
then
act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$
end
Event Define_Security_Rule ⟨ordinary⟩ $\widehat{=}$
extends Define_Security_Rule
any
rio
aio
vio
cor
cio
$perm$
where
grd1: $rio \in RiO1 \land aio \in AiO \land vio \in ViO \land cio \in CiO \land cor \in COR \land perm \in PERMISSION$
grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \land vio = v \mapsto org2 \land cio = c \mapsto org3 \Rightarrow org1 = org2 \land org2 = org3$
grd3: $perm \notin dom(PRA1) \land perm \notin dom(PAA1) \land perm \notin dom(PVA1) \land perm \notin dom(PCA1) \land perm \notin dom(PCxA1)$
grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$
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: $PCxA1 := PCxA1 \cup \{perm \mapsto cio\}$
end
Event Assign_Resource_to_View ⟨ordinary⟩ $\widehat{=}$
extends Assign_Resource_to_View
any
r
vio
where
grd1: $r \in RESOURCE \land vio \in ViO1$
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: $v \in VIEW \land org \in ORG$
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 Can_Request_Access ⟨ordinary⟩ $\widehat{=}$
any
e
a
o
where
grd1: $e \in EMPLOYEE \land a \in ACTION \land o \in RESOURCE$
grd2: $\exists u, r, v, p, org, act, c, rio, aio, vio, cio \cdot (e \mapsto u) \in EA \land (u \mapsto org) \in OU \land rio = (r \mapsto org) \land rio \in RiO \land (u \mapsto rio) \in UR \land (p \mapsto rio) \in PRA \land vio = (v \mapsto org) \land (o \mapsto vio) \in RV \land (p \mapsto vio) \in PVA \land aio = (act \mapsto org) \land (p \mapsto aio) \in PAA \land (a \mapsto vio) \in AV \land (a \mapsto aio) \in AA \land cio = (c \mapsto org) \land (p \mapsto cio) \in PCxA$

then
skip
end
END

MACHINE m9

Request emission

REFINES m8

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
CiO1
Access_Requested

INVARIANTS

inv1: $Access\_Requested \subseteq \mathbb{N}_1 \times EMPLOYEE \times ACTION \times RESOURCE \times COR \times \mathbb{N}$

A request is constitued by a time, the emitter, the action, the resource, the chain of approval, delay.
NB: the chain of approval is copied from the security rule.

EVENTS

Initialisation ⟨extended⟩

begin

act1: $CiO := \varnothing$
act2: $root :\in ORG \nrightarrow UNIT$
act3: $OU :\in UNIT \nrightarrow ORG$
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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $Access\_Requested := \varnothing$

end

Event Concrete_Model_Generation ⟨ordinary⟩ $\widehat{=}$
extends 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: $Approver := Approver1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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⟩ $\widehat{=}$

extends Assign_Approver

any

ou

cor

where

grd1: $ou \in OU1 \land cor \in COR$

grd2: $cor \mapsto ou \notin Approver1$

grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

end

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

extends Define_Security_Rule

any

rio

aio

vio

cor

cio

$perm$

where

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

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

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

grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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

end

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

extends Assign_Resource_to_View

any

r

vio

where

grd1: $r \in RESOURCE \land vio \in ViO1$
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: $v \in VIEW \land org \in ORG$
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 Can_Request_Access
any
e

a
o
t
cor

where

grd1: $e \in EMPLOYEE \land a \in ACTION \land o \in RESOURCE \land t \in \mathbb{N}_1$

grd3: $cor \in COR$

grd4: $\forall e1, a1, o1, t1, cor1, d1 \cdot t1 \mapsto e1 \mapsto a1 \mapsto o1 \mapsto cor1 \mapsto d1 \in Access\_Requested \Rightarrow t > t1$

grd2: $\exists u, r, v, p, org, act, c, rio, aio, vio, cio \cdot e \mapsto u \in EA \land u \mapsto org \in OU \land rio = (r \mapsto org) \land rio \in RiO \land u \mapsto rio \in UR \land p \mapsto rio \in PRA \land vio = (v \mapsto org) \land vio \in ViO \land o \mapsto vio \in RV \land (p \mapsto vio) \in PVA \land aio = (act \mapsto org) \land (p \mapsto aio) \in PAA \land a \mapsto vio \in AV \land (a \mapsto aio) \in AA \land cio = (c \mapsto org) \land (p \mapsto cio) \in PCxA \land (p \mapsto cor) \in PCA$

then

act1: $Access\_Requested := Access\_Requested \cup \{t \mapsto e \mapsto a \mapsto o \mapsto cor \mapsto GLOBAL\_DEADLINE\}$

end

END

MACHINE m10

Add time to request and add request approval event

REFINES m9

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
CiO1
Access_Requested
Request_Treated

INVARIANTS

inv1: $Request\_Treated \subseteq \mathbb{N}_1 \times Access\_Requested \times EMPLOYEE$

An approval is constitued of a time, the request, and the approver.

EVENTS

Initialisation ⟨extended⟩

begin

act1: $CiO := \varnothing$
act2: $root :\in ORG \nrightarrow UNIT$
act3: $OU :\in UNIT \nrightarrow ORG$

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $Request\_Treated := \varnothing$

end

Event Concrete_Model_Generation ⟨ordinary⟩ $\widehat{=}$
extends 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: $Approver := Approver1$

end

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

extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

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

extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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⟩ $\widehat{=}$
extends Assign_Approver

any

ou
cor

where

grd1: $ou \in OU1 \land cor \in COR$
grd2: $cor \mapsto ou \notin Approver1$
grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

end

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

any

rio
aio
vio
cor
cio
$perm$

where

grd1: $rio \in RiO1 \land aio \in AiO \land vio \in ViO \land cio \in CiO \land cor \in COR \land perm \in PERMISSION$
grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \land vio = v \mapsto org2 \land cio = c \mapsto org3 \Rightarrow org1 = org2 \land org2 = org3$
grd3: $perm \notin dom(PRA1) \land perm \notin dom(PAA1) \land perm \notin dom(PVA1) \land perm \notin dom(PCA1) \land perm \notin dom(PCxA1)$
grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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

end

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

any

r

vio

where

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

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: $v \in VIEW \land org \in ORG$

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⟩ $\widehat{=}$

extends Request_Access

any

e
a
o
t
cor

where

grd1: $e \in EMPLOYEE \land a \in ACTION \land o \in RESOURCE \land t \in \mathbb{N}_1$
grd3: $cor \in COR$
grd4: $\forall e1, a1, o1, t1, cor1, d1 \cdot t1 \mapsto e1 \mapsto a1 \mapsto o1 \mapsto cor1 \mapsto d1 \in Access\_Requested \Rightarrow t > t1$
grd2: $\exists u, r, v, p, org, act, c, rio, aio, vio, cio \cdot e \mapsto u \in EA \land u \mapsto org \in OU \land rio = (r \mapsto org) \land rio \in RiO \land u \mapsto rio \in UR \land p \mapsto rio \in PRA \land vio = (v \mapsto org) \land vio \in ViO \land o \mapsto vio \in RV \land (p \mapsto vio) \in PVA \land aio = (act \mapsto org) \land (p \mapsto aio) \in PAA \land a \mapsto vio \in AV \land (a \mapsto aio) \in AA \land cio = (c \mapsto org) \land (p \mapsto cio) \in PCxA \land (p \mapsto cor) \in PCA$

then

act1: $Access\_Requested := Access\_Requested \cup \{t \mapsto e \mapsto a \mapsto o \mapsto cor \mapsto GLOBAL\_DEADLINE\}$

end

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

any

r
s
t

where

grd1: $r \in Access\_Requested \land t \in \mathbb{N}_1$
grd2: $\forall e, a, o, t0, cor, d \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto cor \mapsto d \Rightarrow t > t0 \land e \neq s \land (\exists u, org \cdot cor \mapsto (u \mapsto org) \in Approver \land s \mapsto u \in EA)$
The approver should be member of the request's command chain
grd3: $\forall t1, r1, s1 \cdot t1 \mapsto r1 \mapsto s1 \in Request\_Treated \Rightarrow t > t1 \land t1 \mapsto r \mapsto s \notin Request\_Treated$
approve once per approver
grd4: $\forall u, u1, t1, s1 \cdot s \mapsto u \in EA \land s1 \mapsto u1 \in EA \land t1 < t \land t1 \mapsto r \mapsto s1 \in Request\_Treated \Rightarrow u \neq u1$

approve once per unit

then

act1: $Request\_Treated := Request\_Treated \cup \{t \mapsto r \mapsto s\}$

end

END

MACHINE m11

This machine adds time constraints to requests and approval

REFINES m10

SEES c0

VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
CiO1
Access_Requested
Request_Treated
time
at
PDA permission deadline assingment
Discarded_Request
First_Approver
Next_Approver
Last_Approver

INVARIANTS

inv1: $time \in \mathbb{N}$

inv2: $at \subseteq \mathbb{N}$
inv3: $at \neq \varnothing \Rightarrow time \leq min(at)$
inv4: $PDA \in PERMISSION \pfun \mathbb{N}$
inv5: $Discarded\_Request \subseteq Access\_Requested$
inv6: $First\_Approver \in COR \pfun UNIT$
inv7: $Next\_Approver \subseteq COR \times UNIT \times UNIT$
inv8: $Last\_Approver \in COR \pfun UNIT$

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $Request\_Treated := \varnothing$
act41: $time := 0$
act42: $at := \varnothing$
act43: $PDA := \varnothing$
act44: $Discarded\_Request := \varnothing$
act45: $First\_Approver := \varnothing$
act46: $Last\_Approver := \varnothing$
act47: $Next\_Approver := \varnothing$

end

Event Concrete_Model_Generation ⟨ordinary⟩ $\widehat{=}$
extends 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: $Approver := Approver1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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⟩ $\widehat{=}$

extends Assign_Approver

any

ou

cor

where

grd1: $ou \in OU1 \land cor \in COR$

grd2: $cor \mapsto ou \notin Approver1$

grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$

then

act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$

end

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

refines Define_Security_Rule

any

rio

aio

vio

cor
cio
perm

where

grd1: $rio \in RiO1 \land aio \in AiO \land vio \in ViO \land cio \in CiO \land cor \in COR \land perm \in PERMISSION$
grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \land vio = v \mapsto org2 \land cio = c \mapsto org3 \Rightarrow org1 = org2 \land org2 = org3$
grd3: $perm \notin dom(PRA1) \land perm \notin dom(PAA1) \land perm \notin dom(PVA1) \land perm \notin dom(PCA1) \land perm \notin dom(PCxA1)$
grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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: $r \in RESOURCE \land vio \in ViO1$
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: $v \in VIEW \land org \in ORG$
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
cor
d

where

grd1: $e \in EMPLOYEE \land a \in ACTION \land o \in RESOURCE \land t \in \mathbb{N}_1$
grd6: $d \in \mathbb{N}$
grd5: $t > time$
grd3: $cor \in COR$
grd4: $\forall e1, a1, o1, t1, cor1, d1 \cdot t1 \mapsto e1 \mapsto a1 \mapsto o1 \mapsto cor1 \mapsto d1 \in Access\_Requested \Rightarrow t > t1$
grd2: $\exists u, r, v, p, org, act, c, rio, aio, vio, cio \cdot e \mapsto u \in EA \land u \mapsto org \in OU \land rio = (r \mapsto org) \land rio \in RiO \land u \mapsto rio \in UR \land p \mapsto rio \in PRA \land vio = (v \mapsto org) \land vio \in ViO \land o \mapsto vio \in RV \land (p \mapsto vio) \in PVA \land aio = (act \mapsto org) \land (p \mapsto aio) \in PAA \land a \mapsto vio \in AV \land (a \mapsto aio) \in AA \land cio = (c \mapsto org) \land (p \mapsto cio) \in PCxA \land (p \mapsto cor) \in PCA \land p \mapsto d \in PDA$

then

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

end

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

any

r
s
t

where

grd1: $r \in Access\_Requested \land t \in \mathbb{N}_1$
grd2: $\forall e, a, o, t0, cor, d \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto cor \mapsto d \Rightarrow t > t0 \land e \neq s \land (t - t0 \leq d) \land (\exists u, org \cdot cor \mapsto (u \mapsto org) \in Approver \land s \mapsto u \in EA)$
The approver should be member of the request's command chain
grd3: $\forall t1, r1, s1 \cdot t1 \mapsto r1 \mapsto s1 \in Request\_Treated \Rightarrow t > t1 \land t1 \mapsto r \mapsto s \notin Request\_Treated$
approve once per approver
grd4: $\forall u, u1, t1, s1 \cdot s \mapsto u \in EA \land s1 \mapsto u1 \in EA \land t1 < t \land t1 \mapsto r \mapsto s1 \in Request\_Treated \Rightarrow u \neq u1$

approve once per unit

then
act1: $Request\_Treated := Request\_Treated \cup \{t \mapsto r \mapsto s\}$
end
Event tick_tock ⟨ordinary⟩ $\widehat{=}$
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⟩ $\widehat{=}$
any
p
d
where
grd1: $p \in PERMISSION \land d \in \mathbb{N}$
then
act1: $PDA := PDA \lhd\!\!+ \{p \mapsto d\}$
end
Event Assign_First_Approver ⟨ordinary⟩ $\widehat{=}$
any
cor
u
where
grd1: $cor \mapsto u \notin First\_Approver$
then
act1: $First\_Approver := First\_Approver \cup \{cor \mapsto u\}$
end
Event Assign_Last_Approver ⟨ordinary⟩ $\widehat{=}$
any
cor
u
where
grd1: $cor \mapsto u \notin Last\_Approver$
then
act1: $Last\_Approver := Last\_Approver \cup \{cor \mapsto u\}$
end
Event Assign_Next_Approver ⟨ordinary⟩ $\widehat{=}$
any
cor
u1
u2
where
grd1: $cor \mapsto u1 \mapsto u2 \notin Next\_Approver$
grd2: $cor \mapsto u2 \notin First\_Approver$
grd3: $cor \mapsto u1 \in First\_Approver \lor (\exists u0 \cdot cor \mapsto u0 \mapsto u1 \in Next\_Approver)$
then
act1: $Next\_Approver := Next\_Approver \cup \{cor \mapsto u1 \mapsto u2\}$
end
END

MACHINE m12
REFINES m11
SEES c0
VARIABLES

Approver
PCA
root
OU
RiO
UH
PRA
EA
ViO
AiO
UR
PAA
PVA
CiO
PCxA
RV
AV
AA
root1
UH1
OU1
UR1
RiO1
EA1
Approver1
PRA1
PAA1
PVA1
PCA1
PCxA1
ViO1
RV1
AiO1
AA1
AV1
CiO1
Access_Requested
Request_Treated
time
at
PDA permission deadline assingment
Discarded_Request
First_Approver
Next_Approver
Last_Approver
Dist
PDistA

INVARIANTS

inv1: $Dist \subseteq UNIT \times UNIT \times \mathbb{N}$
inv2: $PDistA \in PERMISSION \pfun \mathbb{N}$

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: $Approver := \varnothing$
act24: $UR1 := \varnothing$
act25: $RiO1 := \varnothing$
act26: $EA1 := \varnothing$
act27: $Approver1 := \varnothing$
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: $Request\_Treated := \varnothing$
act41: $time := 0$
act42: $at := \varnothing$
act43: $PDA := \varnothing$
act44: $Discarded\_Request := \varnothing$
act45: $First\_Approver := \varnothing$
act46: $Last\_Approver := \varnothing$
act47: $Next\_Approver := \varnothing$
act48: $Dist := \varnothing$
act49: $PDistA := \varnothing$

end

Event Concrete_Model_Generation ⟨ordinary⟩ $\widehat{=}$
extends 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: $Approver := Approver1$

end

Event Assign_Oragnization_Root ⟨ordinary⟩ $\widehat{=}$
extends 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: $u \notin ran(root1)$

then

act1: $root1 := root1 \cup \{org \mapsto u\}$

end

Event Add_Unit_Hierarchy ⟨ordinary⟩ $\widehat{=}$
extends 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: $\forall e \cdot e \mapsto u2 \in EA1 \Rightarrow e \mapsto u1 \notin EA1$

then

act1: $UH1 := UH1 \cup \{u1 \mapsto u2\}$

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⟩ $\widehat{=}$
extends Assign_Approver
any
ou
cor
where
grd1: $ou \in OU1 \land cor \in COR$
grd2: $cor \mapsto ou \notin Approver1$
grd3: $\forall u1, org1 \cdot ou = u1 \mapsto org1 \Rightarrow (\forall u2, org2 \cdot u2 \mapsto org2 \in Approver1[\{cor\}] \Rightarrow org1 = org2)$
then
act1: $Approver1 := Approver1 \cup \{cor \mapsto ou\}$
end
Event Define_Security_Rule ⟨ordinary⟩ $\widehat{=}$
extends Define_Security_Rule
any
rio
aio
vio
cor
cio
$perm$
where

grd1: $rio \in RiO1 \land aio \in AiO \land vio \in ViO \land cio \in CiO \land cor \in COR \land perm \in PERMISSION$
grd2: $\forall a, v, c, org1, org2, org3 \cdot aio = a \mapsto org1 \land vio = v \mapsto org2 \land cio = c \mapsto org3 \Rightarrow org1 = org2 \land org2 = org3$
grd3: $perm \notin dom(PRA1) \land perm \notin dom(PAA1) \land perm \notin dom(PVA1) \land perm \notin dom(PCA1) \land perm \notin dom(PCxA1)$
grd4: $\forall r, org \cdot cio = r \mapsto org \Rightarrow (\forall u1, org1 \cdot u1 \mapsto org1 \in Approver[\{cor\}] \Rightarrow org1 = org)$

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: $r \in RESOURCE \land vio \in ViO1$
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: $v \in VIEW \land org \in ORG$
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⟩ $\widehat{=}$

extends Request_Access

any

e

a

o

t

cor

d

where

grd1: $e \in EMPLOYEE \land a \in ACTION \land o \in RESOURCE \land t \in \mathbb{N}_1$

grd6: $d \in \mathbb{N}$

grd5: $t > time$

grd3: $cor \in COR$

grd4: $\forall e1, a1, o1, t1, cor1, d1 \cdot t1 \mapsto e1 \mapsto a1 \mapsto o1 \mapsto cor1 \mapsto d1 \in Access\_Requested \Rightarrow t > t1$

grd2: $\exists u, r, v, p, org, act, c, rio, aio, vio, cio \cdot e \mapsto u \in EA \land u \mapsto org \in OU \land rio = (r \mapsto org) \land rio \in RiO \land u \mapsto rio \in UR \land p \mapsto rio \in PRA \land vio = (v \mapsto org) \land vio \in ViO \land o \mapsto vio \in RV \land (p \mapsto vio) \in PVA \land aio = (act \mapsto org) \land (p \mapsto aio) \in PAA \land a \mapsto vio \in AV \land (a \mapsto aio) \in AA \land cio = (c \mapsto org) \land (p \mapsto cio) \in PCxA \land (p \mapsto cor) \in PCA \land p \mapsto d \in PDA$

then

act1: $Access\_Requested := Access\_Requested \cup \{t \mapsto e \mapsto a \mapsto o \mapsto cor \mapsto d\}$

act2: $at := at \cup \{t\}$

end

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

extends Treat_Request

any

r

s

t

where

grd1: $r \in Access\_Requested \land t \in \mathbb{N}_1$

grd2: $\forall e, a, o, t0, cor, d \cdot r = t0 \mapsto e \mapsto a \mapsto o \mapsto cor \mapsto d \Rightarrow t > t0 \land e \neq s \land (t - t0 \leq d) \land (\exists u, org \cdot cor \mapsto (u \mapsto org) \in Approver \land s \mapsto u \in EA)$

The approver should be member of the request's command chain

grd3: $\forall t1, r1, s1 \cdot t1 \mapsto r1 \mapsto s1 \in Request\_Treated \Rightarrow t > t1 \land t1 \mapsto r \mapsto s \notin Request\_Treated$

approve once per approver

grd4: $\forall u, u1, t1, s1 \cdot s \mapsto u \in EA \land s1 \mapsto u1 \in EA \land t1 < t \land t1 \mapsto r \mapsto s1 \in Request\_Treated \Rightarrow u \neq u1$

approve once per unit

then

act1: $Request\_Treated := Request\_Treated \cup \{t \mapsto r \mapsto s\}$

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⟩ $\widehat{=}$
extends Assign_Approval_Deadline
any
p
d
where
grd1: $p \in PERMISSION \land d \in \mathbb{N}$
then
act1: $PDA := PDA \lhd\!\!+ \{p \mapsto d\}$
end
Event Assign_First_Approver ⟨ordinary⟩ $\widehat{=}$
extends Assign_First_Approver
any
cor
u
where
grd1: $cor \mapsto u \notin First\_Approver$
then
act1: $First\_Approver := First\_Approver \cup \{cor \mapsto u\}$
end
Event Assign_Last_Approver ⟨ordinary⟩ $\widehat{=}$
extends Assign_Last_Approver
any
cor
u
where
grd1: $cor \mapsto u \notin Last\_Approver$
then
act1: $Last\_Approver := Last\_Approver \cup \{cor \mapsto u\}$
end
Event Assign_Next_Approver ⟨ordinary⟩ $\widehat{=}$
extends Assign_Next_Approver
any
cor
$u1$
$u2$
where
grd1: $cor \mapsto u1 \mapsto u2 \notin Next\_Approver$
grd2: $cor \mapsto u2 \notin First\_Approver$
grd3: $cor \mapsto u1 \in First\_Approver \lor (\exists u0 \cdot cor \mapsto u0 \mapsto u1 \in Next\_Approver)$
then
act1: $Next\_Approver := Next\_Approver \cup \{cor \mapsto u1 \mapsto u2\}$
end
Event Assign_Permission_Distance ⟨ordinary⟩ $\widehat{=}$
any
p
d
where

grd1: $p \mapsto d \notin PDistA$

then

act1: $PDistA := PDistA \cup \{p \mapsto d\}$

end

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

any

u1

u2

d

where

grd1: $u1 \mapsto u2 \mapsto d \notin Dist$

grd2: $u1 = u2 \Rightarrow d = 0$

then

act1: $Dist := Dist \cup \{u1 \mapsto u2 \mapsto d\}$

end

END