

KORRIGAN : un formalisme et une méthode pour la spécification formelle et structurée de systèmes mixtes

Pascal POIZAT

`Pascal.Poizat@irin.univ-nantes.fr`

Institut de Recherche en Informatique de Nantes

- 1 Spécifications formelles mixtes
- 2 Le modèle des vues de KORRIGAN
- 3 Méthode de spécification pour systèmes mixtes
- 4 ASK : un Atelier pour Spécifier avec KORRIGAN
- 5 Conclusions et perspectives

1 - Spécifications formelles mixtes

- objectifs
- spécification des aspects statiques
- spécification des aspects dynamiques et des compositions
- choix

- systèmes sécuritaires et/ou critiques

Objectifs

- systèmes sécuritaires et/ou critiques
 - ⇒ spécifications **formelles**

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)

spécifications formelles

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)
 - ⇒ spécification mixtes

spécifications formelles

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)
- taille des spécifications, réutilisation

spécifications formelles mixtes

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)
- taille des spécifications, réutilisation
 - spécifications structurées

spécifications formelles mixtes

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)
- taille des spécifications, réutilisation
- monde industriel, utilisateurs non experts

spécifications formelles mixtes structurées

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)
- taille des spécifications, réutilisation
- monde industriel, utilisateurs non experts
 - lisibilité
 - méthode
 - atelier (guides, génération de code, vérification)

spécifications formelles mixtes structurées

Objectifs

- systèmes sécuritaires et/ou critiques
- systèmes complexes : différents aspects (statique, dynamique, composition)
- taille des spécifications, réutilisation
- monde industriel, utilisateurs non experts

spécifications formelles mixtes structurées

+ lisibilité

+ méthode

+ atelier

Spécification des aspects statiques

- approche orientée modèle
(Z, B, VDM)
 - ⇒ concepts plus connus (ensembles, relations, ...)
 - ⇒ moins abstraite
 - ⇒ “industrielle”

Spécification des aspects statiques

- approche orientée modèle
(Z, B, VDM)
 - ⇒ concepts plus connus (ensembles, relations, ...)
 - ⇒ moins abstraite
 - ⇒ “industrielle”
- approche orientée propriétés
(spéc. algébriques, logiques d'ordre supérieur)
 - ⇒ concepts moins courants (algèbres, formules, ...)
 - ⇒ plus expressive, plus abstraite
 - ⇒ outillage plus important (exécutabilité)
 - ⇒ “académique”

Critères concernant aspects dynamiques et composition

- communication
 - ◆ synchrone
 - ◆ asynchrone (synchrone + buffers)

Critères concernant aspects dynamiques et composition

- communication
 - ◆ synchrone
 - ◆ asynchrone (synchrone + buffers)
- temps
 - ◆ logique
 - ◆ physique

Critères concernant aspects dynamiques et composition

- communication
 - ◆ synchrone
 - ◆ asynchrone (synchrone + buffers)
- temps
 - ◆ logique
 - ◆ physique
- concurrence
 - ◆ vraie
 - ◆ entrelacement

Spécification des aspects dynamiques et de la composition

- approche algèbres de processus
(CCS, CSP, Basic LOTOS)
 - ⇒ expressive, abstraite mais peu lisible

Spécification des aspects dynamiques et de la composition

- approche algèbres de processus
(CCS, CSP, Basic LOTOS)
 - ⇒ expressive, abstraite mais peu lisible
- approche logique
(TLA, Unity)
 - ⇒ très expressive, abstraite
 - ⇒ peu structurée et très peu lisible

Spécification des aspects dynamiques et de la composition

- approche algèbres de processus
(CCS, CSP, Basic LOTOS)
 - ⇒ expressive, abstraite mais peu lisible
- approche logique
(TLA, Unity)
 - ⇒ très expressive, abstraite
 - ⇒ peu structurée et très peu lisible
- approche systèmes de transitions
(automates, réseaux de Petri, SDL, Statecharts)
 - ⇒ formalismes graphiques très lisibles
 - ⇒ problèmes d'explosion du nombre d'états/transitions

Spécifications mixtes

- approche hétérogène (plusieurs formalismes)
 - ⇒ plus **expressive**, plus **lisible**
 - ⇒ problèmes de sémantique globale
 - ⇒ **bien adaptée à la spécification**

Spécifications mixtes

- approche hétérogène (plusieurs formalismes)
 - ⇒ plus **expressive**, plus **lisible**
 - ⇒ problèmes de sémantique globale
 - ⇒ **bien adaptée à la spécification**

- approche homogène (un seul formalisme)
 - ⇒ moins expressive, moins lisible
 - ⇒ sémantique globale bien définie
 - ⇒ pas de séparation des aspects
 - ⇒ **bien adaptée à la vérification et à la validation**

Et pour Noël, j'aimerais ...

- statique : **spécifications algébriques** avec réécriture
- dynamique : **systèmes de transitions** avec bon niveau d'abstraction
- composition : **logique temporelle** (réduite) associée aux systèmes de transitions

- approche **hétérogène** pour la définition des briques de base de définition des composants
- approche **unifiée** pour la description des aspects

→ ???

Et pour Noël, j'aimerais ...

- statique : **spécifications algébriques** avec réécriture
- dynamique : **systèmes de transitions** avec bon niveau d'abstraction
- composition : **logique temporelle** (réduite) associée aux systèmes de transitions

- approche **hétérogène** pour la définition des briques de base de définition des composants
- approche **unifiée** pour la description des aspects

➡ modèle des vues de KORRIGAN

2 - Le modèle des vues de KORRIGAN

- un modèle à base de vues
pourquoi et comment ?
- les composants de base
- les compositions
- sémantique
- fil rouge : gestionnaire de mots de passe

Les vues : pourquoi ?

- une brique de base de description des composants
- lisibilité, expressivité, abstraction
- permettre une structuration simple mais expressive des spécifications de façon unifiée par rapport aux différentes structurations
- permettre la définition et la réutilisation de composants par la séparation des aspects

Les vues : comment ? (les composants de base)

- des composants **de base** pour les aspects de base (statique, dynamique)
 - ◆ un **système de transitions** et une **spécification algébrique** associée
 - ◆ liens forts entre le **système de transitions** et la **spécification algébrique**

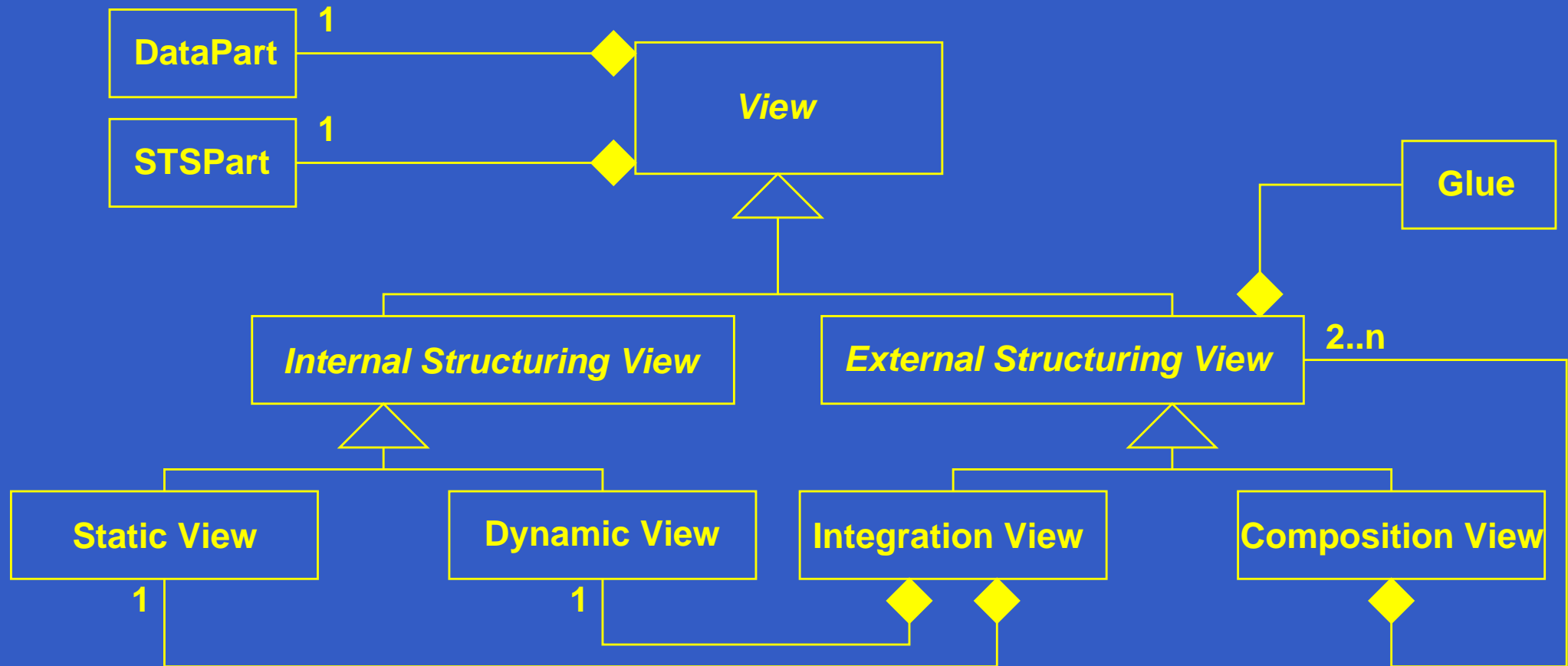
Les vues : comment ? (les composants de base)

- des composants **de base** pour les aspects de base (statique, dynamique)
 - ◆ un **système de transitions** et une **spécification algébrique** associée
 - ◆ liens forts entre le **système de transitions** et la **spécification algébrique**
 - ◆ description d'un niveau d'**abstraction** basé sur des conditions
 - ◆ description des opérations en termes de pré et postconditions sur ces conditions
 - ◆ liens forts entre le **système de transitions** et cette **abstraction**

Les vues : comment ? (la composition)

- des **compositions** pour les autres aspects (intégration, composition parallèle)
 - ◆ faire correspondre statique et dynamique
 - ⇒ **intégration**
 - ◆ faire correspondre les protocoles de communication tout en respectant le masquage de l'information
 - ⇒ **composition parallèle**
 - ◆ unification de ces différentes compositions

Un modèle à base de vues



vue : concept unificateur permettant de spécifier les différents **aspects** des **composants** de façon **structurée**

VIEW T

SPECIFICATION

imports A'

hides \bar{A}

generic on G

variables V

ops Σ

axioms Ax

ABSTRACTION

conditions C

limit conditions Cl

with Φ

initially Φ_0

OPERATIONS

O_i

pre: P

post: Q

VIEW T

SPECIFICATION

imports A'

hides \bar{A}

generic on G

variables V

ops Σ

axioms Ax

ABSTRACTION

conditions C

limit conditions Cl

with Φ

initially Φ_0

OPERATIONS

O_i

pre: P

post: Q

VIEW T

SPECIFICATION

imports A'

hides \bar{A}

generic on G

variables V

ops Σ

axioms Ax

ABSTRACTION

conditions C

limit conditions Cl

with Φ

initially Φ_0

OPERATIONS

O_i

pre: P

post: Q

VIEW T

SPECIFICATION

imports A'

hides \bar{A}

generic on G

variables V

ops Σ

axioms Ax

ABSTRACTION

conditions C

limit conditions Cl

with Φ

initially Φ_0

OPERATIONS

O_i

pre: P

post: Q

Vue en KORRIGAN

VIEW T

SPECIFICATION

imports A'

hides \bar{A}

generic on G

variables V

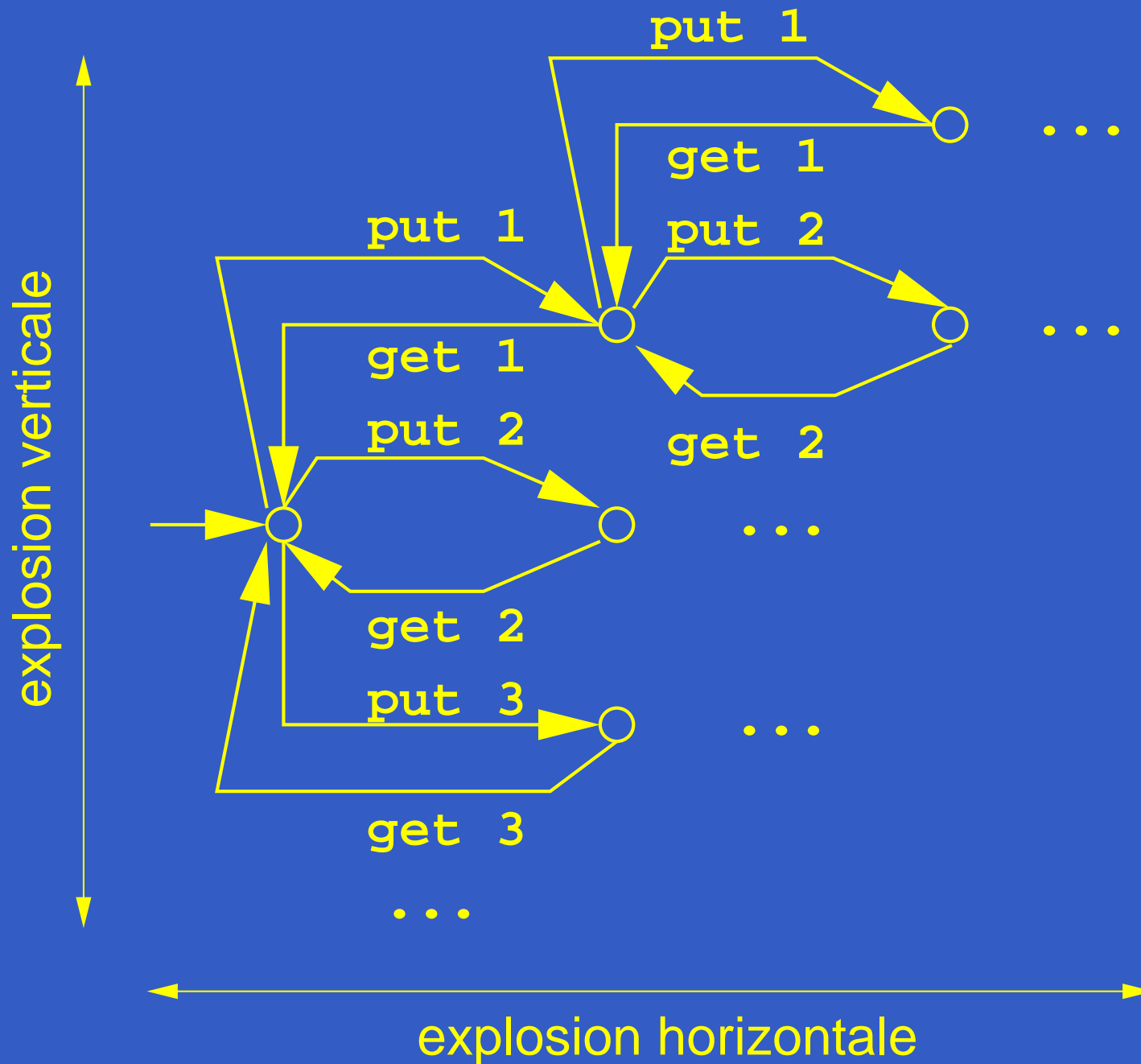
ops Σ

axioms Ax

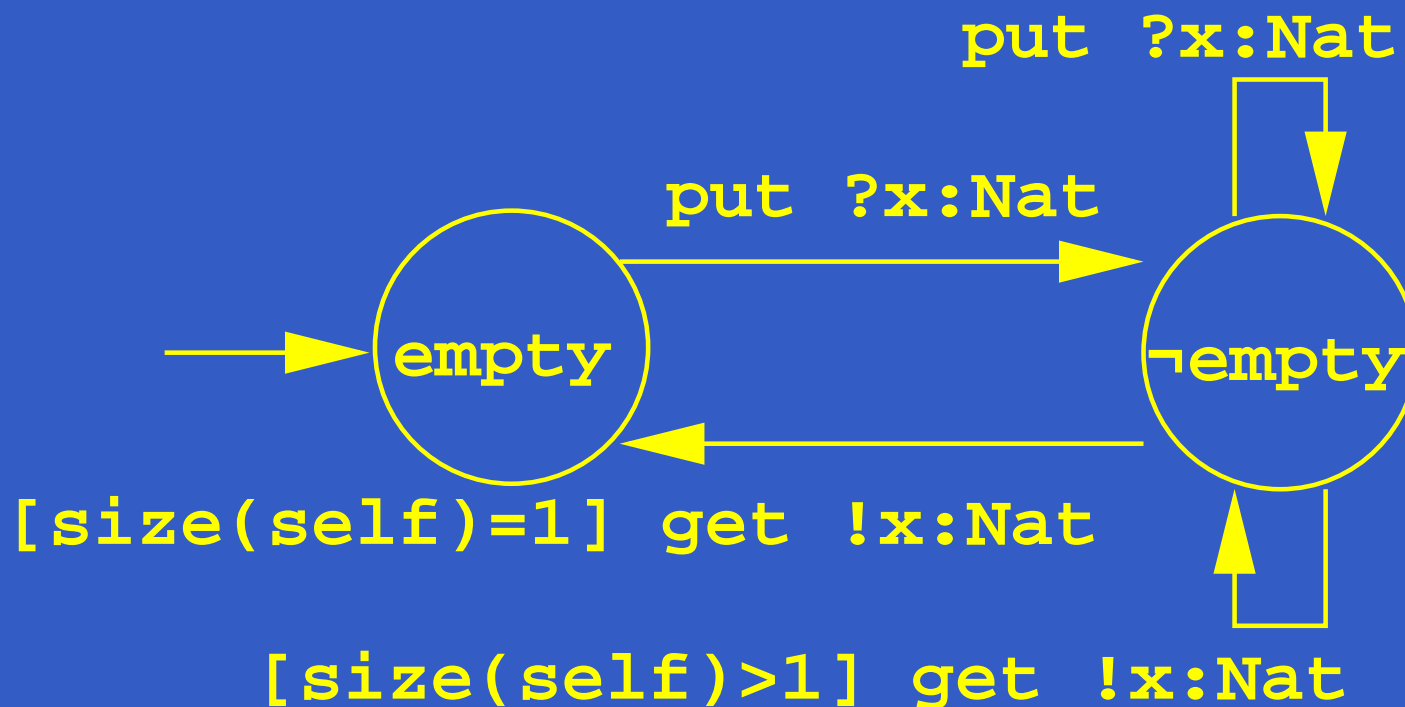
STS

⇒ ???

Système de transitions



Systèmes de transitions abstraits



- abstraction relative à l'explosion horizontale
 - états symboliques
- abstraction relative à l'explosion verticale
 - transitions symboliques

Des systèmes de transitions aux STS

- Graphes de Transitions Symboliques [HL95]
 - ◆ états : un ensemble de variables libres
 - ◆ transitions : garde + **action dynamique** (liaison de variables)
 - ◆ sémantique : liaisons sur le nom des variables
 - ➡ sémantique globale pour CSP, full LOTOS

Des systèmes de transitions aux STS

- Graphes de Transitions Symboliques [HL95]
 - ◆ états : un ensemble de variables libres
 - ◆ transitions : garde + **action dynamique** (liaison de variables)
 - ◆ sémantique : liaisons sur le nom des variables
 - ➡ sémantique globale pour CSP, full LOTOS
- Types Abstraites Graphiques [And95]
 - ◆ **liaison automate / spécification algébrique**
 - ◆ états : une classe d'équivalence, un terme
 - ◆ transitions : garde + opération (terme)
 - ◆ sémantique : axiomes

Systèmes de Transitions Symboliques (STS)

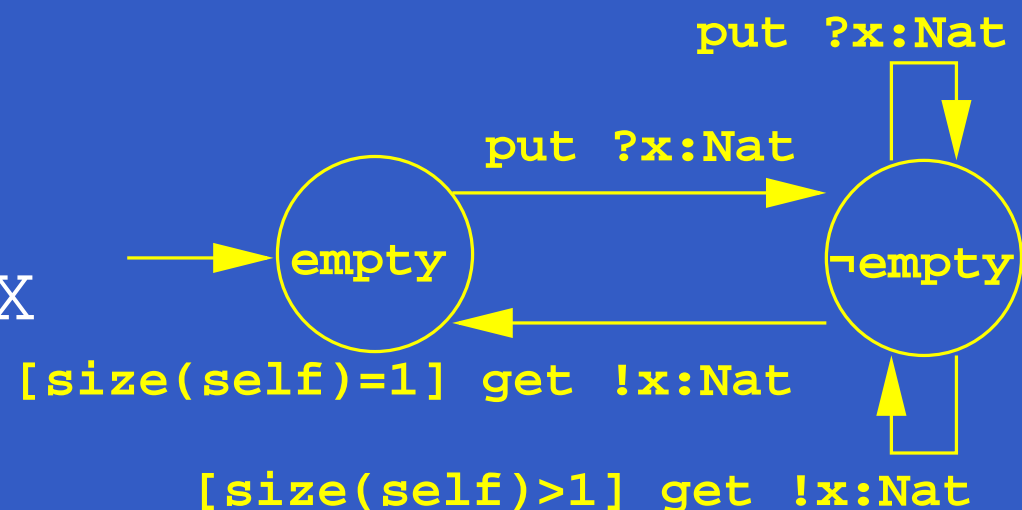
extension des TAG

- STS basé sur une abstraction
- états : conditions
- opérations : pré / postconditions
- 2 gardes (construction)
- signatures dynamiques

⇒ $p \ ?x_i : T_i \text{ from } x : PIdX$

⇒ $p \ !v_i : T_i \text{ to } x : PIdX$

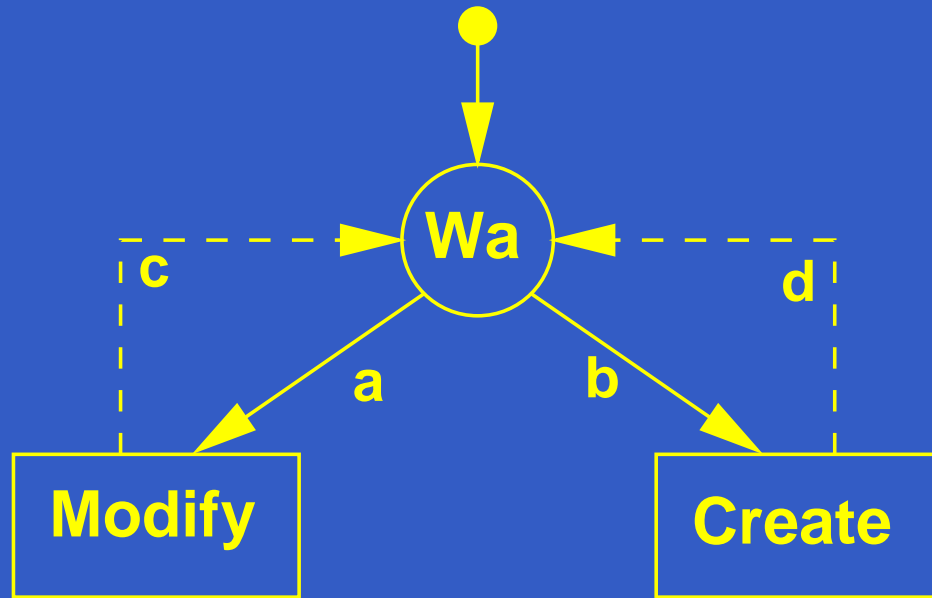
⇒ $p \ ?x_i : T_i \ !v_i : T_i$



- composition plus générale et orientation composants dynamiques

Le gestionnaire de mots de passe (dynamique)

aspect dynamique : protocole de communication



a modify
from u:PIdUser

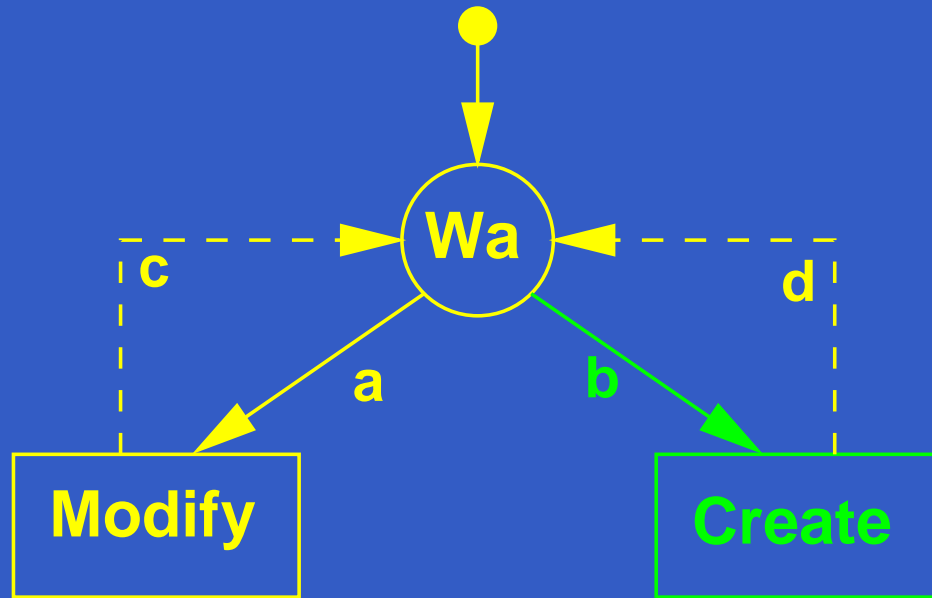
b create ?u:PIdUser
from root:PIdRoot

c [true]

d [true]

Le gestionnaire de mots de passe (dynamique)

aspect dynamique : protocole de communication



a modify
from u:PIdUser

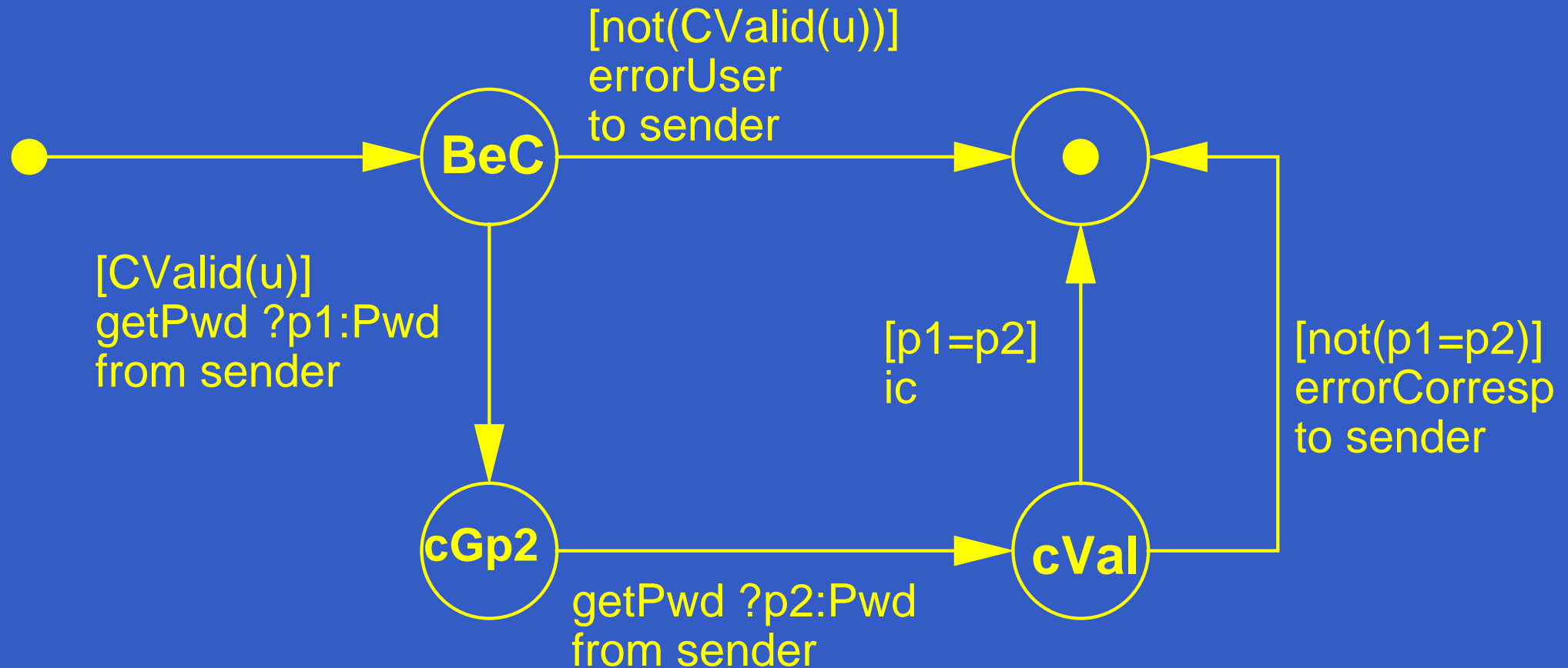
b create ?u:PIdUser
from root:PIdRoot

c [true]

d [true]

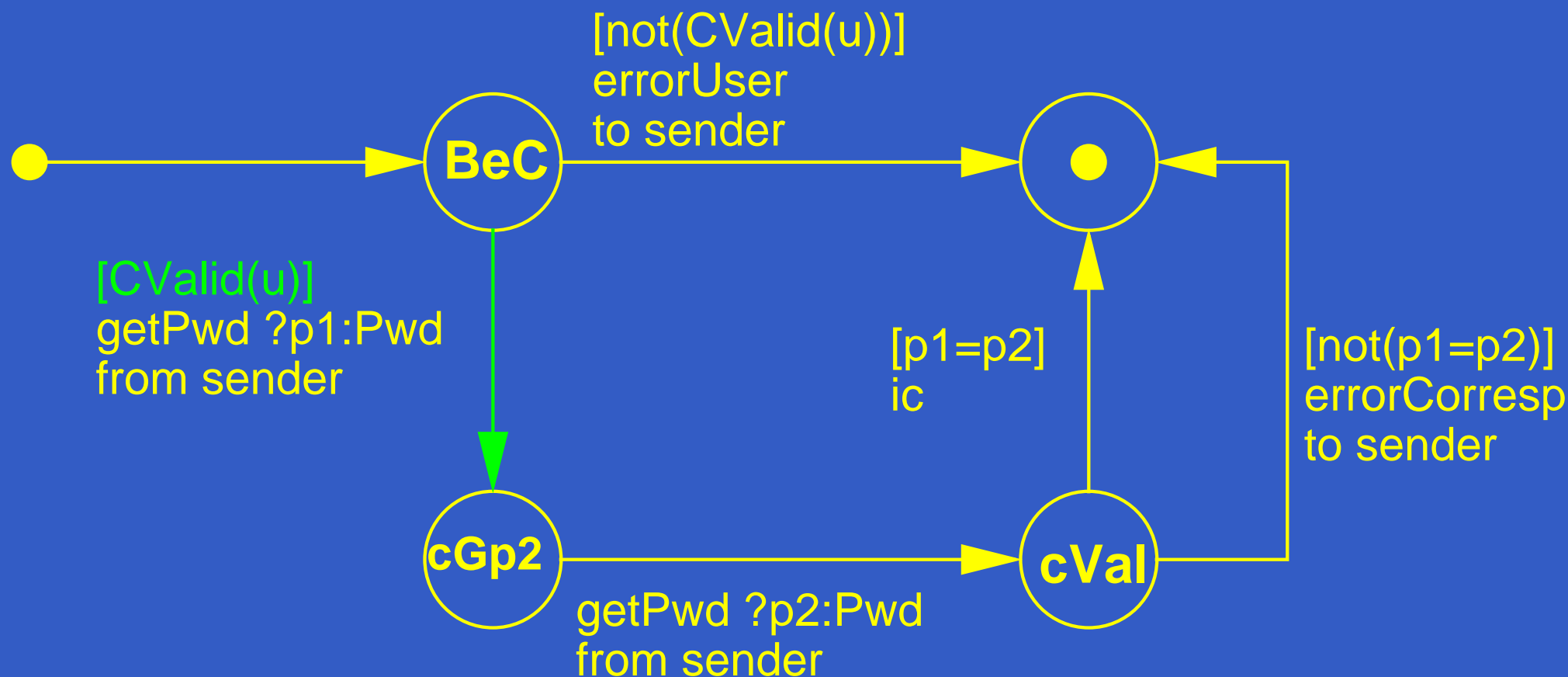
Le gestionnaire de mots de passe (dynamique)

aspect dynamique : protocole de communication



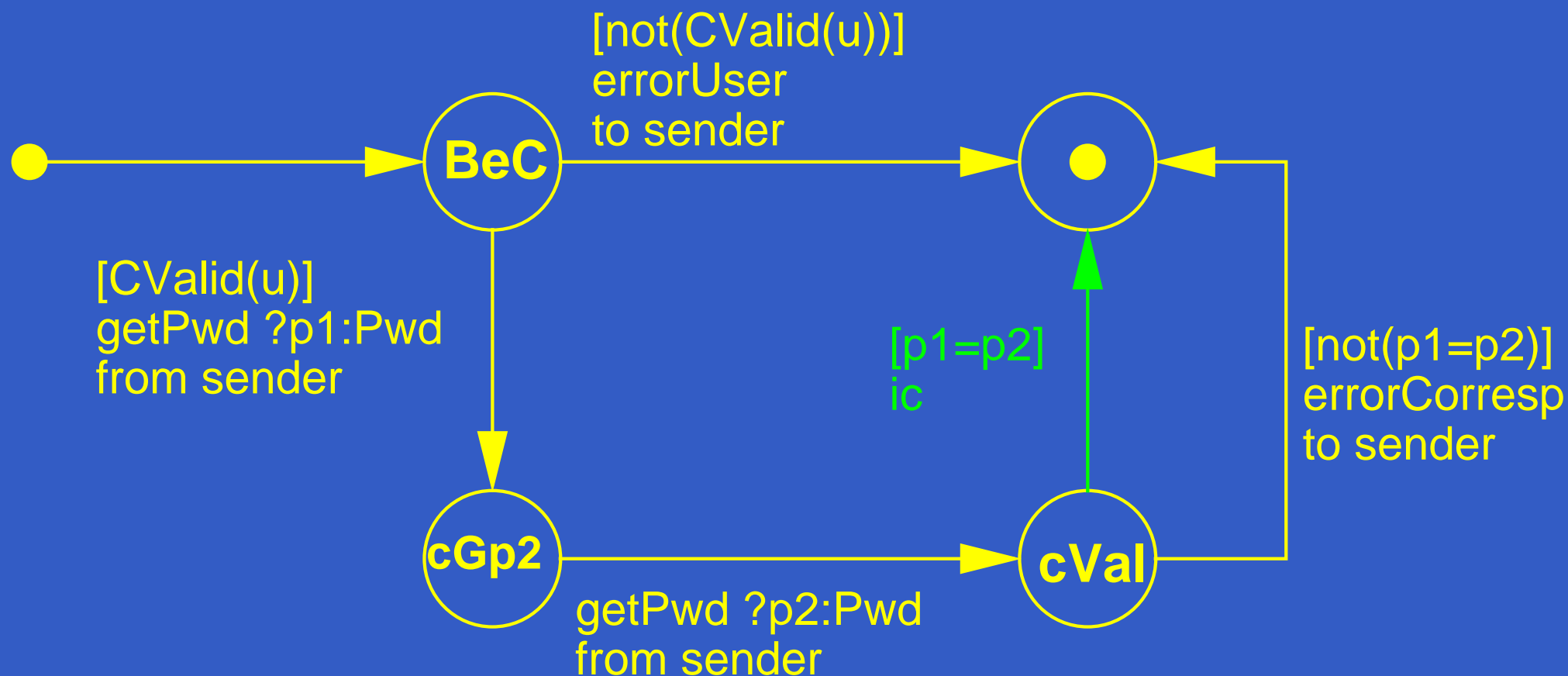
Le gestionnaire de mots de passe (dynamique)

aspect dynamique : protocole de communication



Le gestionnaire de mots de passe (dynamique)

aspect dynamique : protocole de communication



Le gestionnaire de mots de passe (statique)

aspect statique : fichier `/etc/passwd`

STATIC VIEW StaticPasswordManager (SPM)

SPECIFICATION

`imports Boolean, UserId, Pwd`

`ops`

`empty : → SPM`

`add : SPM, UserId, Pwd → SPM`

`modify : SPM, UserId, Pwd → SPM`

`declared : SPM, UserId → Boolean`

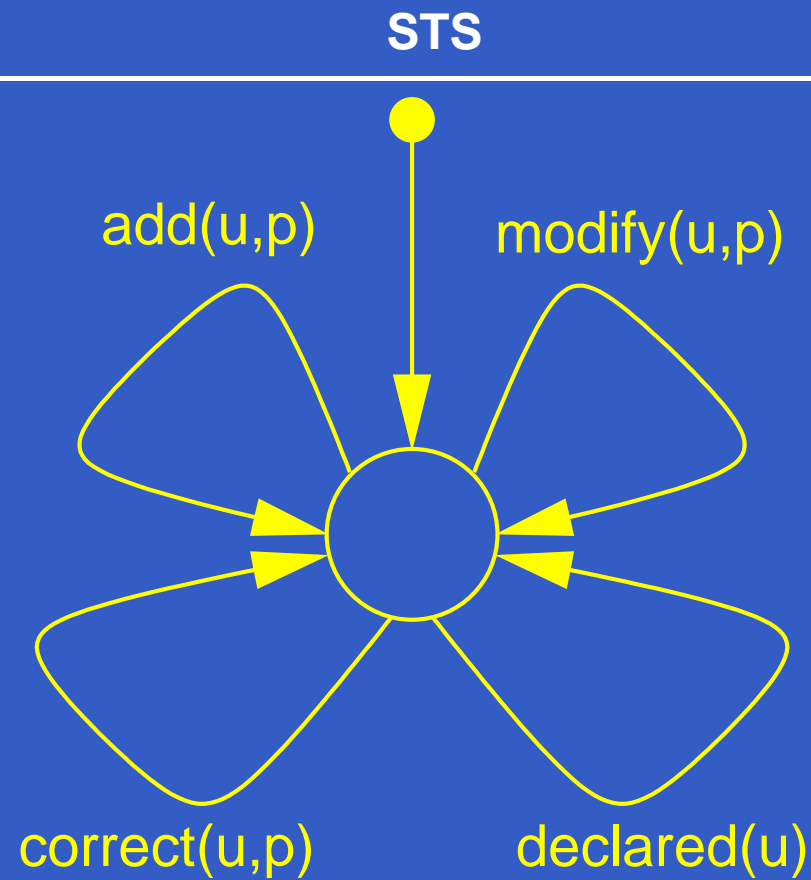
`correct : SPM, UserId, Pwd → Boolean`

`...`

Le gestionnaire de mots de passe (statique)

aspect statique : fichier `/etc/passwd`

STATIC VIEW StaticPasswordManager (SPM)



Oui, mais ...

Pourquoi une vue pour les aspects statiques ?

Pourquoi une vue pour les aspects statiques ?

- ⇒ pour l'unification des concepts de composition
- ⇒ intégration "=" composition parallèle

Oui, mais ...

Pourquoi une vue pour les aspects statiques ?

- ⇒ pour l'unification des concepts de composition
- ⇒ intégration “=” composition parallèle

Mais alors pourquoi pas simplement une vue ?

- ⇒ aspect statique “=” partie données
- ⇒ aspect dynamique “=” partie STS

Oui, mais ...

Pourquoi une vue pour les aspects statiques ?

- ⇒ pour l'unification des concepts de composition
- ⇒ intégration “=” composition parallèle

Mais alors pourquoi pas simplement une vue ?

- ⇒ aspect statique “=” partie données
- ⇒ aspect dynamique “=” partie STS

Pour la **séparation des aspects**
et la **réutilisation des composants** !

Composition

- ensemble de sous-composants
- collage

Composition

- ensemble de sous-composants
- collage

Comment faire ?

Composition

- ensemble de sous-composants
- collage

Comment faire ?

- ⇒ coller les STS des sous-composants
- états initiaux, états (exclusions)
 - ⇒ formules d'états
- transitions (communications, synchronisations)
 - ⇒ formules de transitions
- gardes / opérations
 - ⇒ axiomes

Formules de transitions

$$\frac{t=s \xrightarrow{[g_t] \quad l_t \quad [g'_t]} s', l \sim l_t, g_t \Rightarrow g, g'_t \Rightarrow g'}{\Gamma, t \models [g]l[g']}$$

PROP_t

$$\frac{\{x \mapsto t'\} \in \Gamma, t \sim t'}{\Gamma, t \models x}$$

IDENT_t

$$\frac{\Gamma \cup \{x \mapsto t\}, t \models \Psi_1}{\Gamma, t \models \exists x. \Psi_1}$$

BIND_t

$$\overline{\Gamma, t \models true}$$

TRUE_t

$$\overline{\Gamma, t \not\models false}$$

FALSE_t

$$\frac{\Gamma, t \not\models \Psi_1}{\Gamma, t \models \neg \Psi_1}$$

NOT_t

$$\frac{\Gamma, t \models \Psi_1 \wedge \Gamma, t \models \Psi_2}{\Gamma, t \models \Psi_1 \wedge \Psi_2}$$

AND_t

$$\frac{t=s \xrightarrow{l} s', \Gamma, s' \models \Phi_1}{\Gamma, t \models > \Phi_1}$$

TARGET

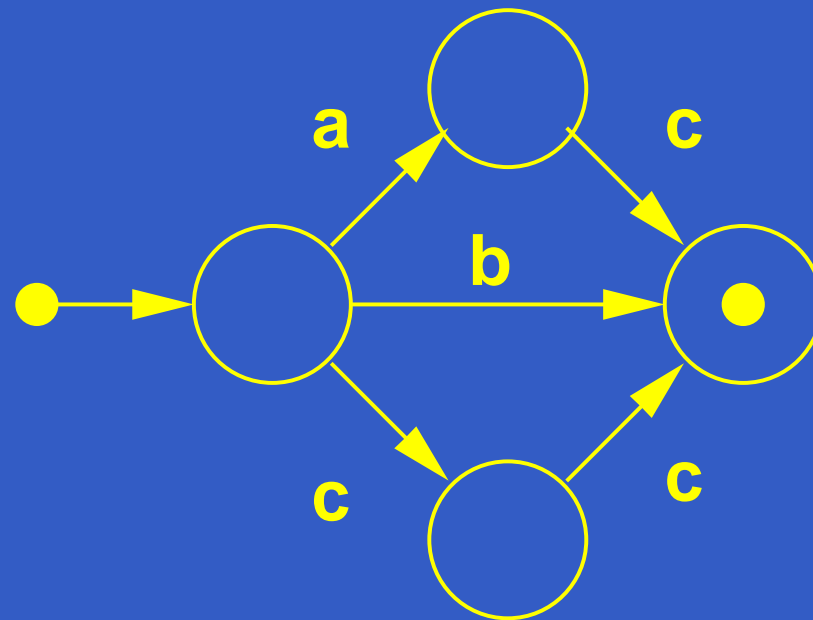
$$\frac{\exists i. t' \in t, \Gamma, t' \models \psi_1}{\Gamma, t \models i. \psi_1}$$

INDEX_t

→ formules d'états, sur le même principe

Formules de transitions

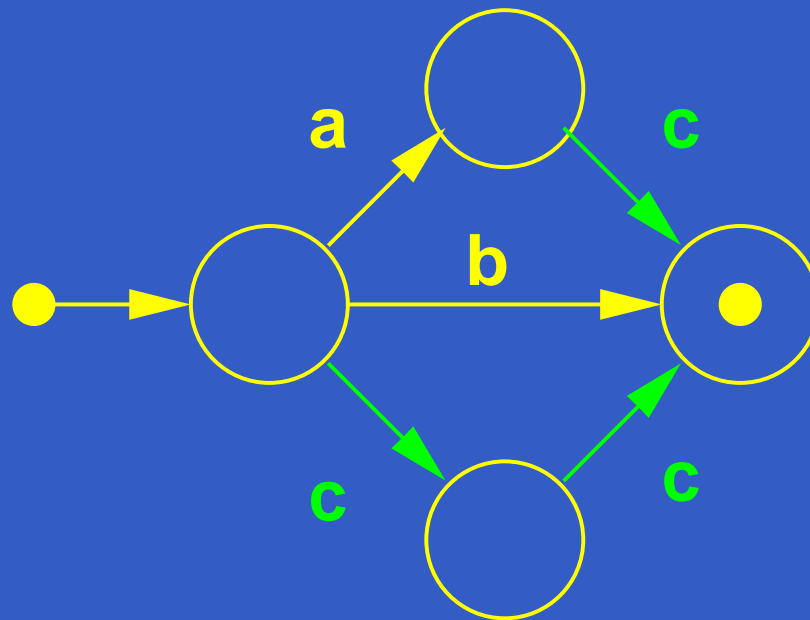
$$\frac{t=s \xrightarrow{l} s', \Gamma, s' \models \Phi_1}{\Gamma, t \models \triangleright \Phi_1} \quad \textit{TARGET}$$



$$c \wedge \triangleright \bullet$$

Formules de transitions

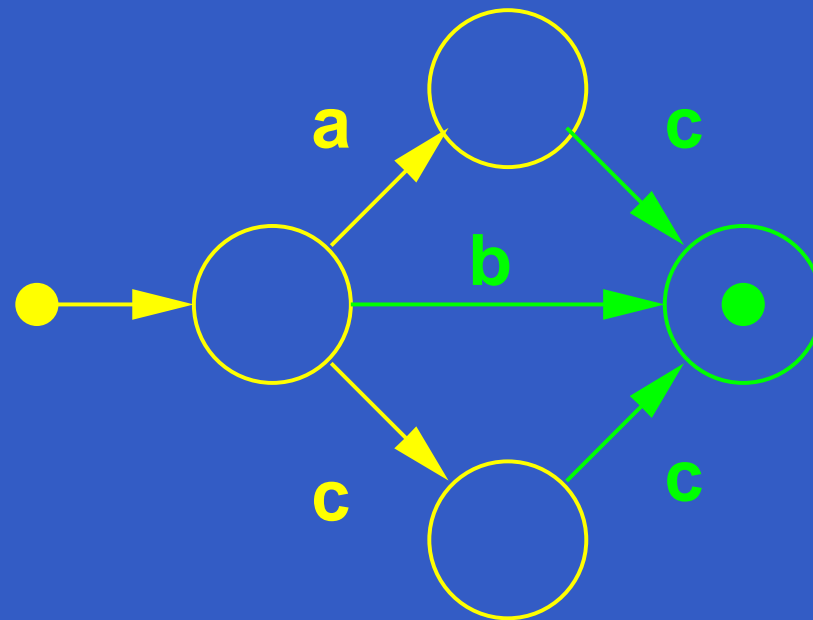
$$\frac{t=s \xrightarrow{l} s', \Gamma, s' \models \Phi_1}{\Gamma, t \models \triangleright \Phi_1} \quad \text{TARGET}$$



$$c \wedge \triangleright \bullet$$

Formules de transitions

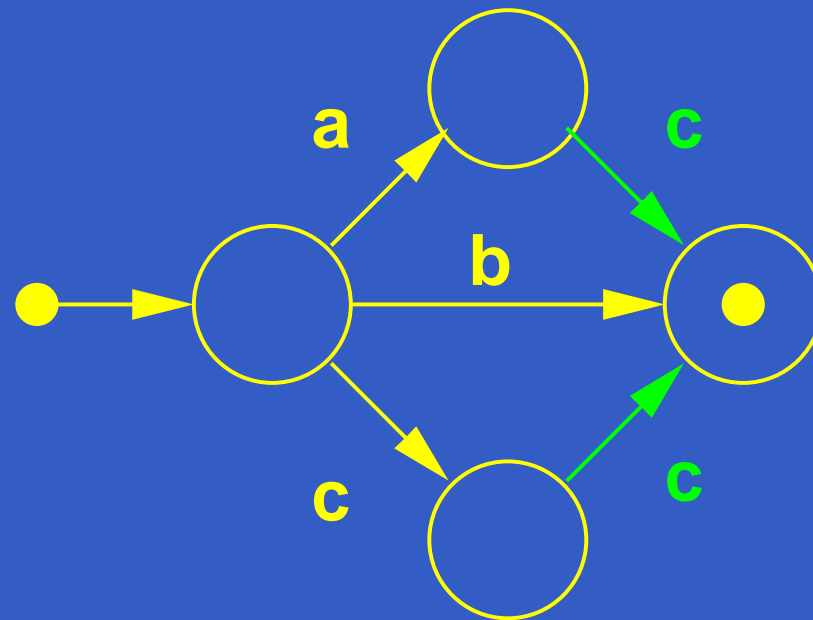
$$\frac{t=s \xrightarrow{l} s', \Gamma, s' \models \Phi_1}{\Gamma, t \models \triangleright \Phi_1} \quad TARGET$$



$$c \wedge \triangleright \bullet$$

Formules de transitions

$$\frac{t=s \xrightarrow{l} s', \Gamma, s' \models \Phi_1}{\Gamma, t \models \triangleright \Phi_1} \quad \textit{TARGET}$$



$c \wedge \triangleright \bullet$

Vues de composition : les ESV

EXTERNAL STRUCTURING VIEW T

SPECIFICATION

imports A'

generic on G

variables V

COMPOSITION δ

is

$id_i : Obj_i[I_i]$

axioms Ax_{Θ}

with Φ, Ψ **initially** Φ_0

Vues de composition : les ESV

EXTERNAL STRUCTURING VIEW T

SPECIFICATION

imports A'

generic on G

variables V

COMPOSITION δ

is

$id_i : Obj_i[I_i]$

axioms Ax_{Θ}

with Φ, Ψ **initially** Φ_0

Vues de composition : les ESV

EXTERNAL STRUCTURING VIEW T

SPECIFICATION

imports A'

generic on G

variables V

COMPOSITION δ

is

$id_i : Obj_i[I_i]$

axioms Ax_{Θ}

with Φ, Ψ initially Φ_0

Vues de composition : les ESV

EXTERNAL STRUCTURING VIEW T

SPECIFICATION

imports A'
generic on G
variables V

COMPOSITION δ

is

$id_i : Obj_i[I_i]$

axioms Ax_{Θ}

with Φ, Ψ initially Φ_0

- Ax_{Θ} : ensemble d'axiomes
- Φ : ensemble de formules d'états
- Φ_0 : formule d'états
- Ψ : couples de formules de transitions

Vues de composition : les ESV

EXTERNAL STRUCTURING VIEW T

SPECIFICATION

imports A'
generic on G
variables V

COMPOSITION δ

is

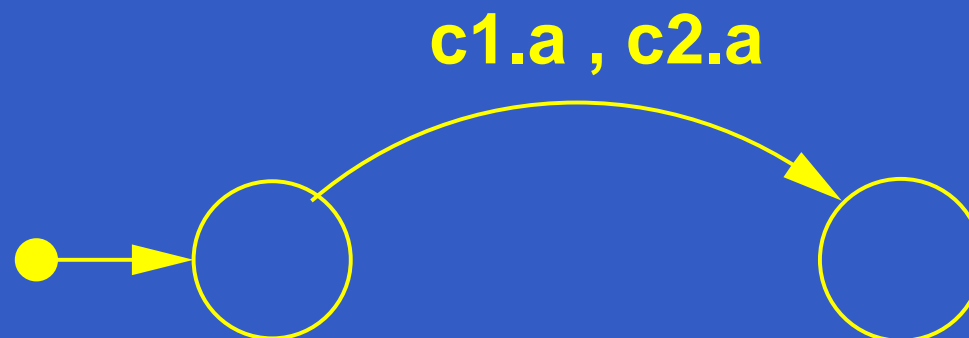
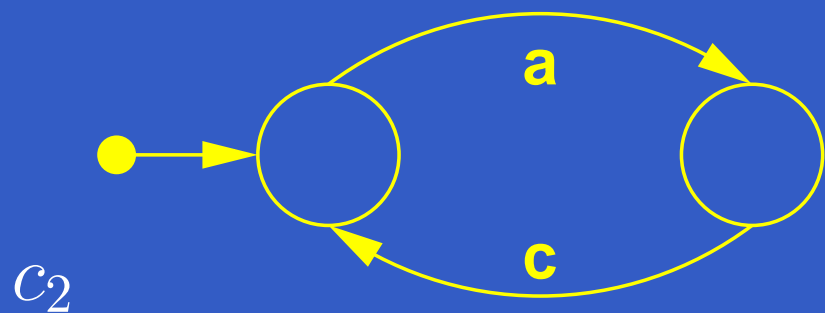
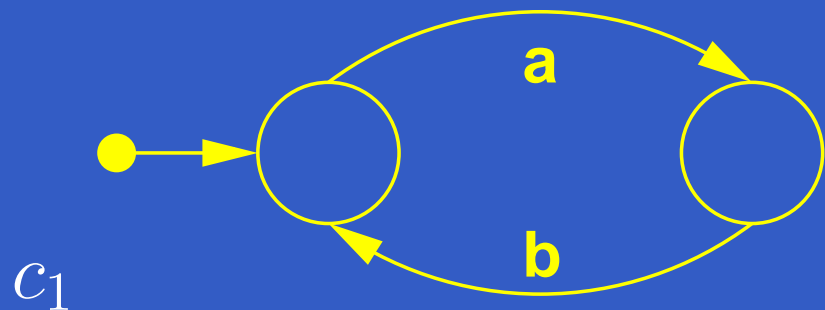
$id_i : Obj_i[I_i]$

axioms Ax_{Θ}

with Φ, Ψ initially Φ_0

- Ax_{Θ} : ensemble d'axiomes
- Φ : ensemble de formules d'états
- Φ_0 : formule d'états
- Ψ : couples de formules de transitions
- δ : que faire des transitions non collées par Ψ ?

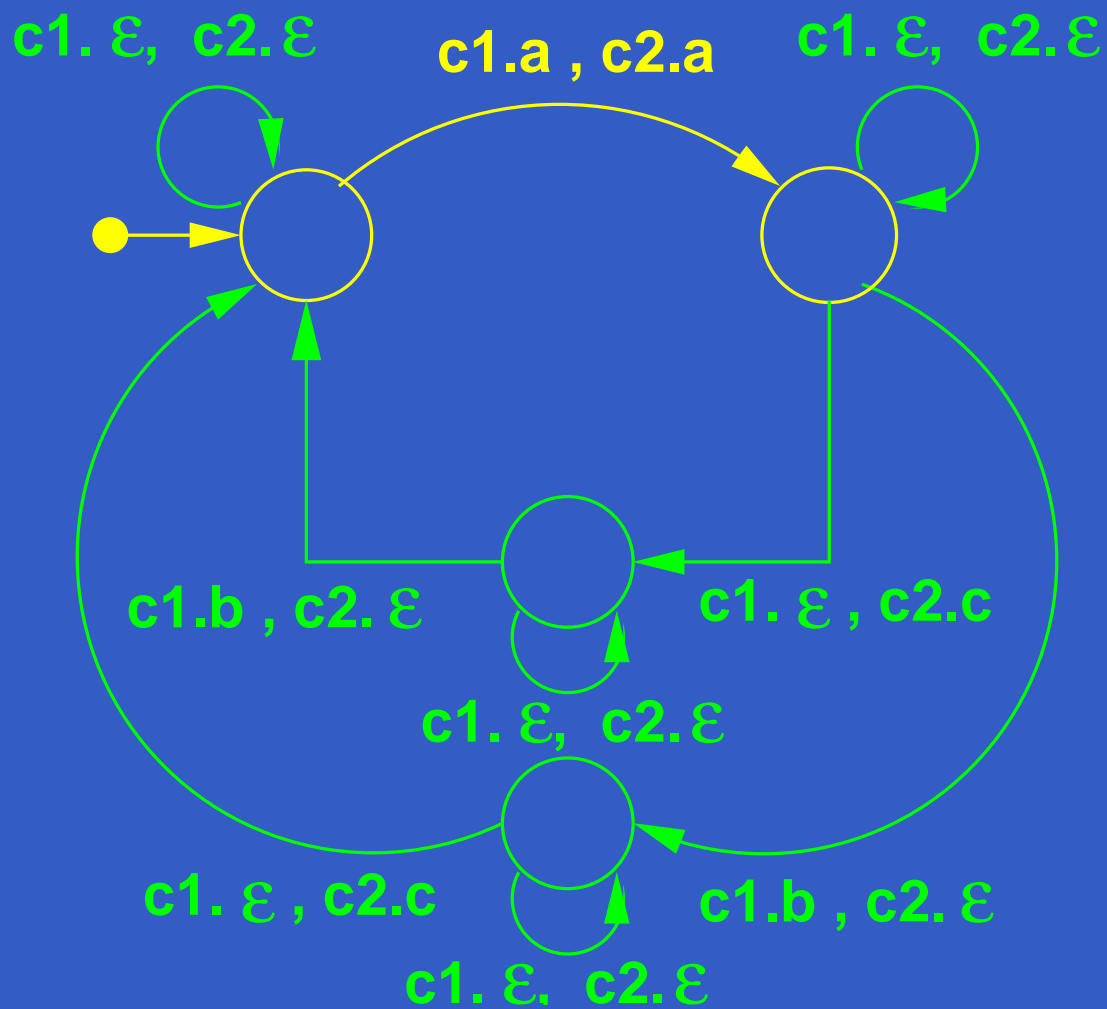
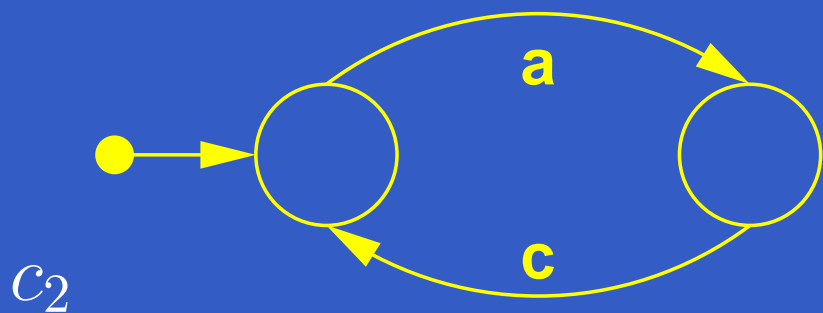
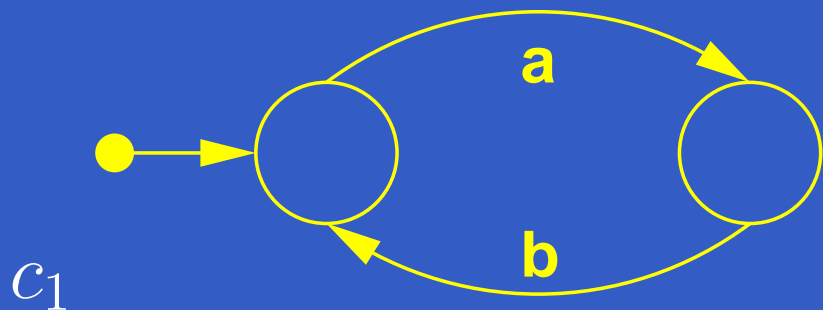
LOOSE , ALONE et KEEP



LOOSE

$$\Psi = \{(c_1.a, c_2.a)\}$$

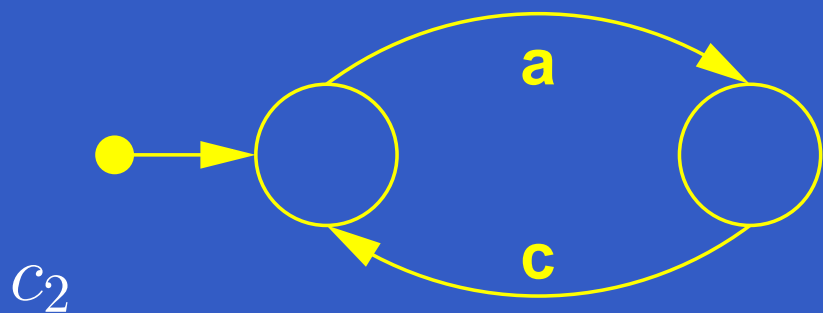
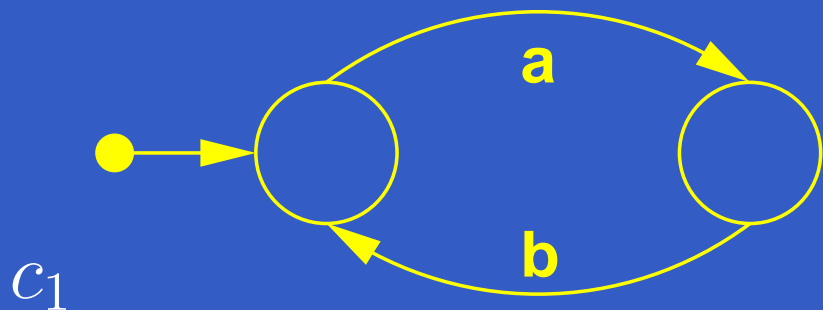
LOOSE , ALONE et KEEP



LOOSE + ALONE

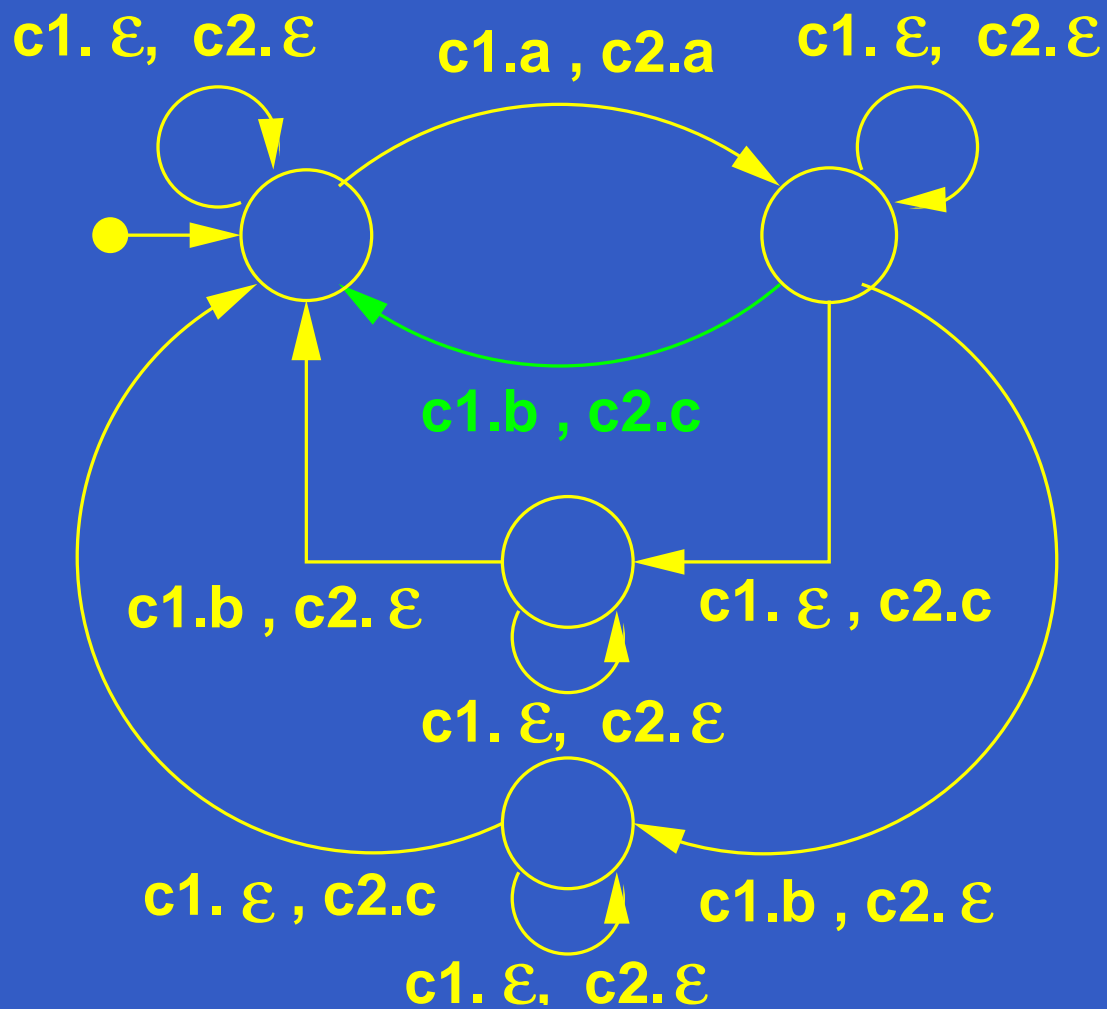
$$\Psi = \{(c_1.a, c_2.a)\}$$

LOOSE , ALONE et KEEP

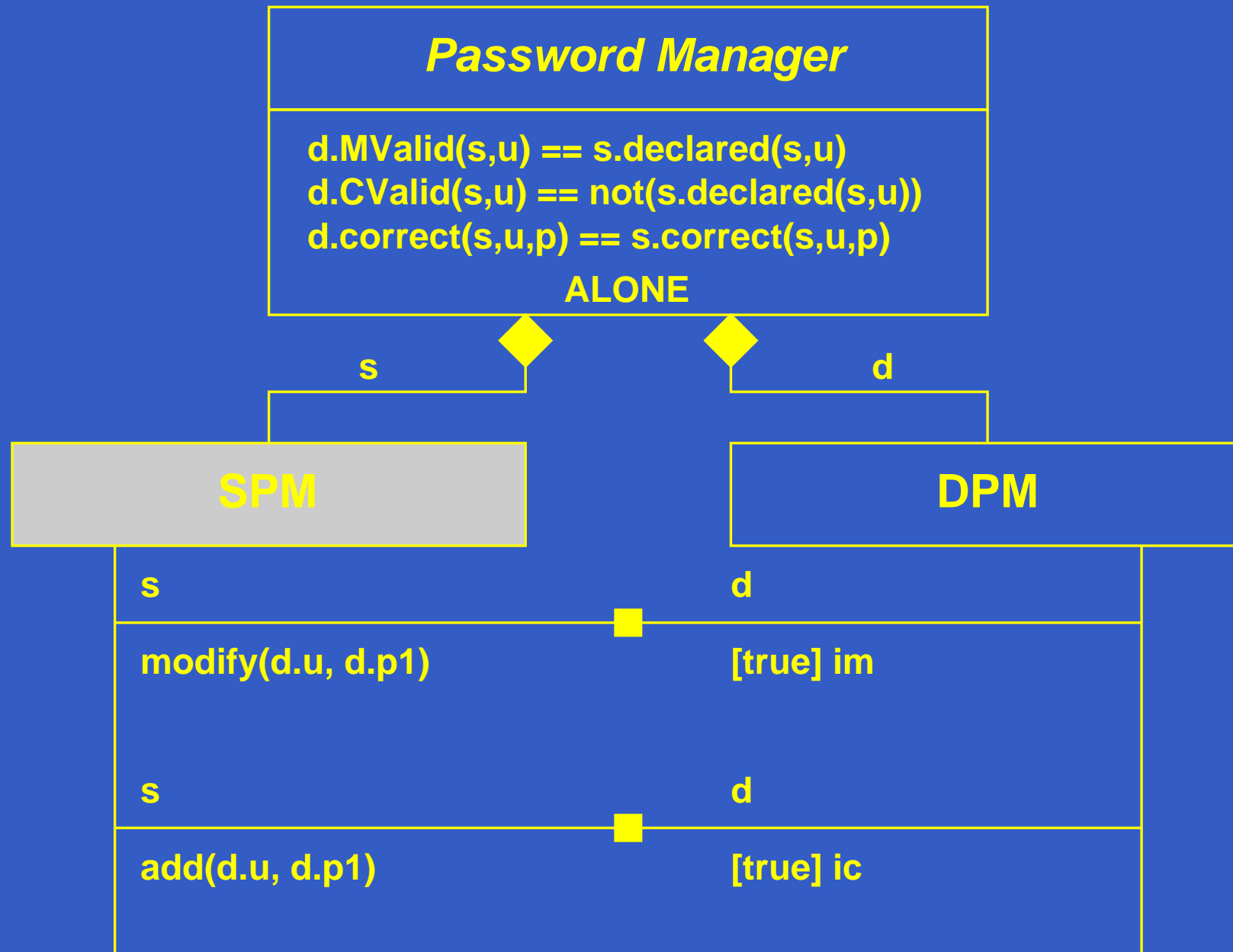


LOOSE + KEEP

$$\Psi = \{(c_1.a, c_2.a)\}$$



Le gestionnaire de mots de passe (intégration)



Le gestionnaire de mots de passe (intégration)

INTEGRATION VIEW Password Manager

COMPOSITION ALONE

is

STATIC s : SPM

DYNAMIC d : DPM

axioms

$d.MValid(s,u) == s.declared(s,u)$

$d.CValid(s,u) == \text{not}(s.declared(s,u))$

$d.correct(s,u,p) == s.correct(s,u,p)$

with true,

{

($d.[true] im$),

$s.modify(d.u,d.p1)$),

($d.[true] ic$),

$s.add(d.u,d.p1)$)

}

initially true

Sémantique : comment ?

Sémantique : comment ?

1. calculer une vue **globale** :

Sémantique : comment ?

1. calculer une vue **globale** :
 - calculer un STS global

Sémantique : comment ?

1. calculer une vue **globale** :
 - calculer un STS global
 - calculer une partie donnée globale

Sémantique : comment ?

1. calculer une vue **globale** :
 - calculer un STS global
 - calculer une partie donnée globale
2. en donner la sémantique

STS global (transitions)

$$t_s = s_s \xrightarrow{[g_s] \ l_s \ [gio_s]} s'_s \in T(Obj_s),$$

$$t_d = s_d \xrightarrow{[g_d] \ l_d \ [gio_d]} s'_d \in T(Obj_d),$$

$$\exists(\psi_{i_s}, \psi_{i_d}) \in \psi \mid t_s \models \psi_{i_s}, t_d \models \psi_{i_d},$$

$$s = \langle s.s_s/d.s_d \rangle, s' = \langle s.s'_s/d.s'_d \rangle,$$

$$g = \langle s.g_s/d.g_d \rangle, gio = \langle s.gio_s/d.gio_d \rangle, l = \langle s.l_s/d.l_d \rangle,$$

$$s \in S, s' \models \phi$$

$$s \xrightarrow{[g] \ l \ [gio]} s' \in T$$

*TRANSACTION*_{LOOSE}

mais aussi *TRANSACTION*_{KEEP} et *TRANSACTION*_{ALONE}

STS global (transitions)

$$t_s = s_s \xrightarrow{[g_s] \ l_s \ [gio_s]} s'_s \in T(Obj_s),$$

$$t_d = s_d \xrightarrow{[g_d] \ l_d \ [gio_d]} s'_d \in T(Obj_d),$$

$$\exists(\psi_{i_s}, \psi_{i_d}) \in \psi \mid t_s \models \psi_{i_s}, t_d \models \psi_{i_d},$$

$$s = \langle s.s_s/d.s_d \rangle, s' = \langle s.s'_s/d.s'_d \rangle,$$

$$g = \langle s.g_s/d.g_d \rangle, gio = \langle s.gio_s/d.gio_d \rangle, l = \langle s.l_s/d.l_d \rangle,$$

$$s \in S, s' \models \phi$$

$$s \xrightarrow{[g] \ l \ [gio]} s' \in T$$

*TRANSACTION*_{LOOSE}

mais aussi *TRANSACTION*_{KEEP} et *TRANSACTION*_{ALONE}

STS global (transitions)

$$t_s = s_s \xrightarrow{[g_s] \ l_s \ [gio_s]} s'_s \in T(Obj_s),$$

$$t_d = s_d \xrightarrow{[g_d] \ l_d \ [gio_d]} s'_d \in T(Obj_d),$$

$$\exists(\psi_{i_s}, \psi_{i_d}) \in \psi \mid t_s \models \psi_{i_s}, t_d \models \psi_{i_d},$$

$$s = \langle s.s_s/d.s_d \rangle, s' = \langle s.s'_s/d.s'_d \rangle,$$

$$g = \langle s.g_s/d.g_d \rangle, gio = \langle s.gio_s/d.gio_d \rangle, l = \langle s.l_s/d.l_d \rangle,$$

$$s \in S, s' \models \phi$$

$$s \xrightarrow{[g] \ l \ [gio]} s' \in T$$

*TRANSACTION*_{LOOSE}

mais aussi *TRANSACTION*_{KEEP} et *TRANSACTION*_{ALONE}

STS global (transitions)

$$t_s = s_s \xrightarrow{[g_s] \ l_s \ [gio_s]} s'_s \in T(Obj_s),$$

$$t_d = s_d \xrightarrow{[g_d] \ l_d \ [gio_d]} s'_d \in T(Obj_d),$$

$$\exists(\psi_{i_s}, \psi_{i_d}) \in \psi \mid t_s \models \psi_{i_s}, t_d \models \psi_{i_d},$$

$$s = \langle s.s_s/d.s_d \rangle, s' = \langle s.s'_s/d.s'_d \rangle,$$

$$g = \langle s.g_s/d.g_d \rangle, gio = \langle s.gio_s/d.gio_d \rangle, l = \langle s.l_s/d.l_d \rangle,$$

$$s \in S, s' \models \phi$$

$$s \xrightarrow{[g] \ l \ [gio]} s' \in T$$

*TRANSACTION*_{LOOSE}

mais aussi *TRANSACTION*_{KEEP} et *TRANSACTION*_{ALONE}

STS global (transitions)

$$t_s = s_s \xrightarrow{[g_s] \ l_s \ [gio_s]} s'_s \in T(Obj_s),$$

$$t_d = s_d \xrightarrow{[g_d] \ l_d \ [gio_d]} s'_d \in T(Obj_d),$$

$$\exists(\psi_{i_s}, \psi_{i_d}) \in \psi \mid t_s \models \psi_{i_s}, t_d \models \psi_{i_d},$$

$$s = \langle s.s_s/d.s_d \rangle, s' = \langle s.s'_s/d.s'_d \rangle,$$

$$g = \langle s.g_s/d.g_d \rangle, gio = \langle s.gio_s/d.gio_d \rangle, l = \langle s.l_s/d.l_d \rangle,$$

$$s \in S, s' \models \phi$$

$$s \xrightarrow{[g] \ l \ [gio]} s' \in T$$

*TRANSACTION*_{LOOSE}

mais aussi *TRANSACTION*_{KEEP} et *TRANSACTION*_{ALONE}

STS global (transitions)

$$t_s = s_s \xrightarrow{[g_s] \ l_s \ [gio_s]} s'_s \in T(Obj_s),$$

$$t_d = s_d \xrightarrow{[g_d] \ l_d \ [gio_d]} s'_d \in T(Obj_d),$$

$$\exists(\psi_{i_s}, \psi_{i_d}) \in \psi \mid t_s \models \psi_{i_s}, t_d \models \psi_{i_d},$$

$$s = \langle s.s_s/d.s_d \rangle, s' = \langle s.s'_s/d.s'_d \rangle,$$

$$g = \langle s.g_s/d.g_d \rangle, gio = \langle s.gio_s/d.gio_d \rangle, l = \langle s.l_s/d.l_d \rangle,$$

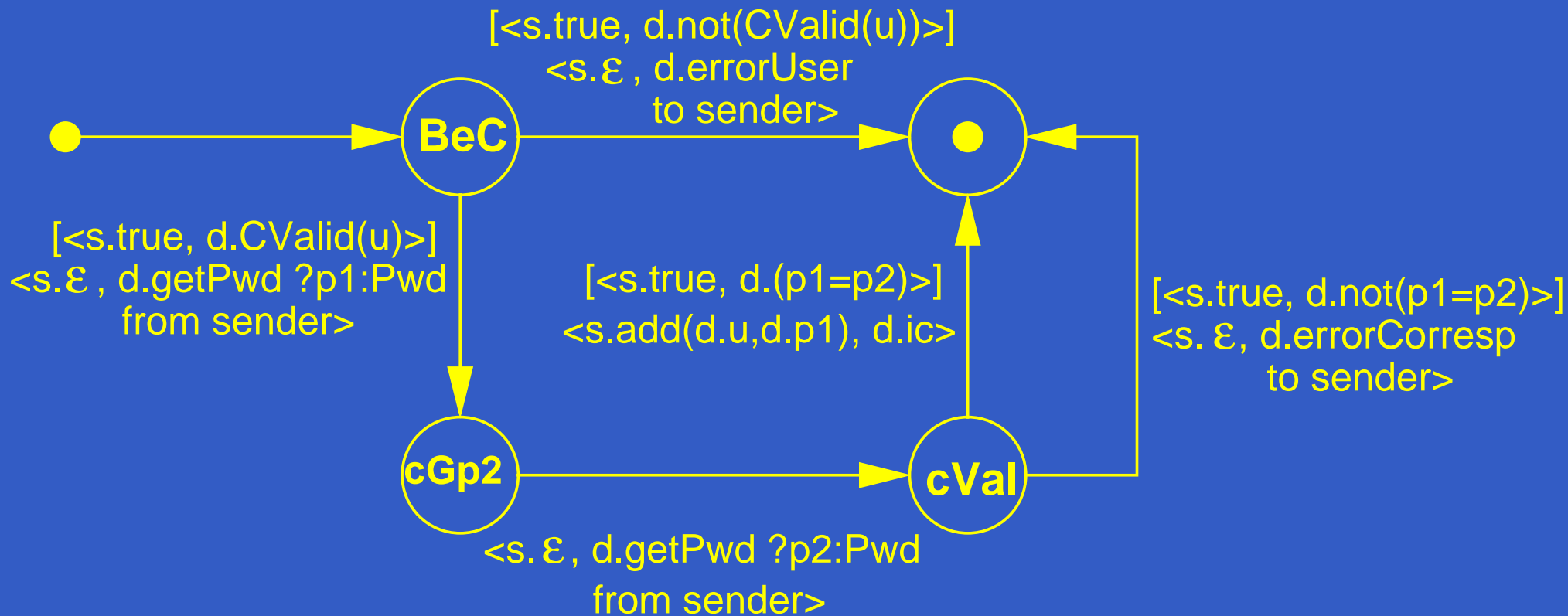
$$s \in S, s' \models \phi$$

$$s \xrightarrow{[g] \ l \ [gio]} s' \in T$$

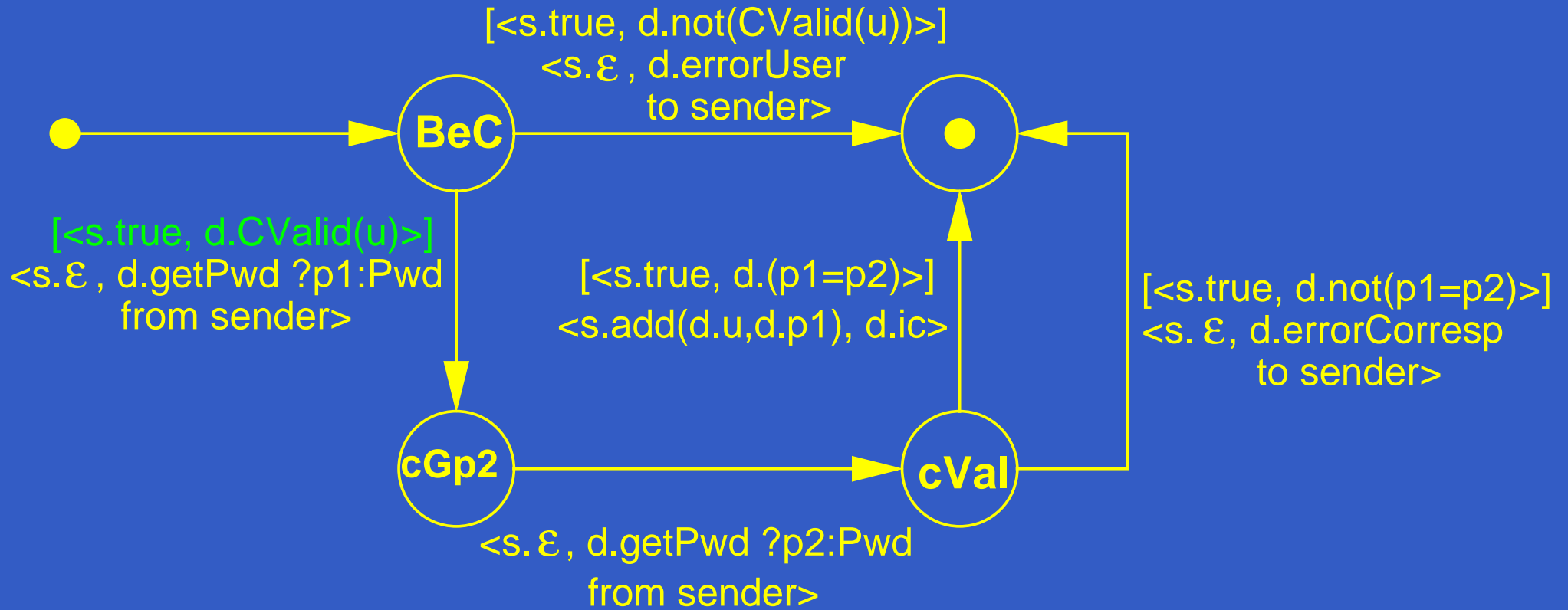
*TRANSACTION*_{LOOSE}

mais aussi *TRANSACTION*_{KEEP} et *TRANSACTION*_{ALONE}

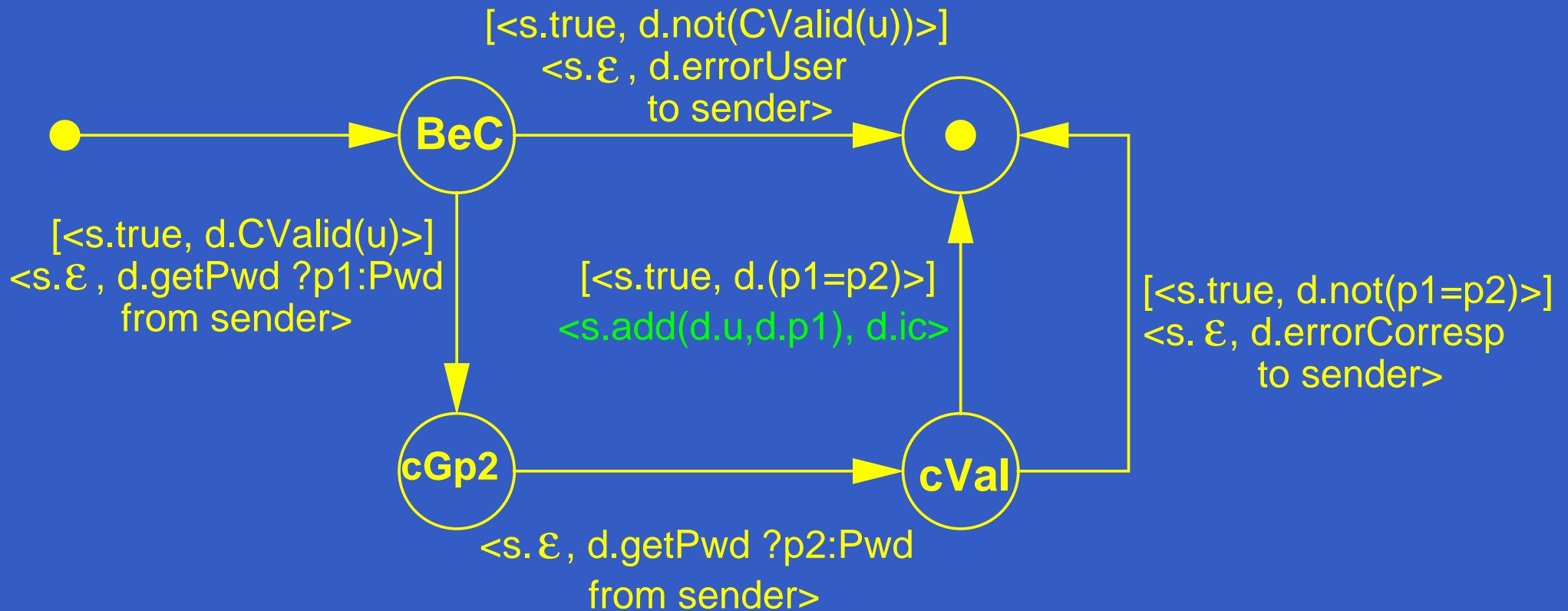
Le gestionnaire de mots de passe (STS global)



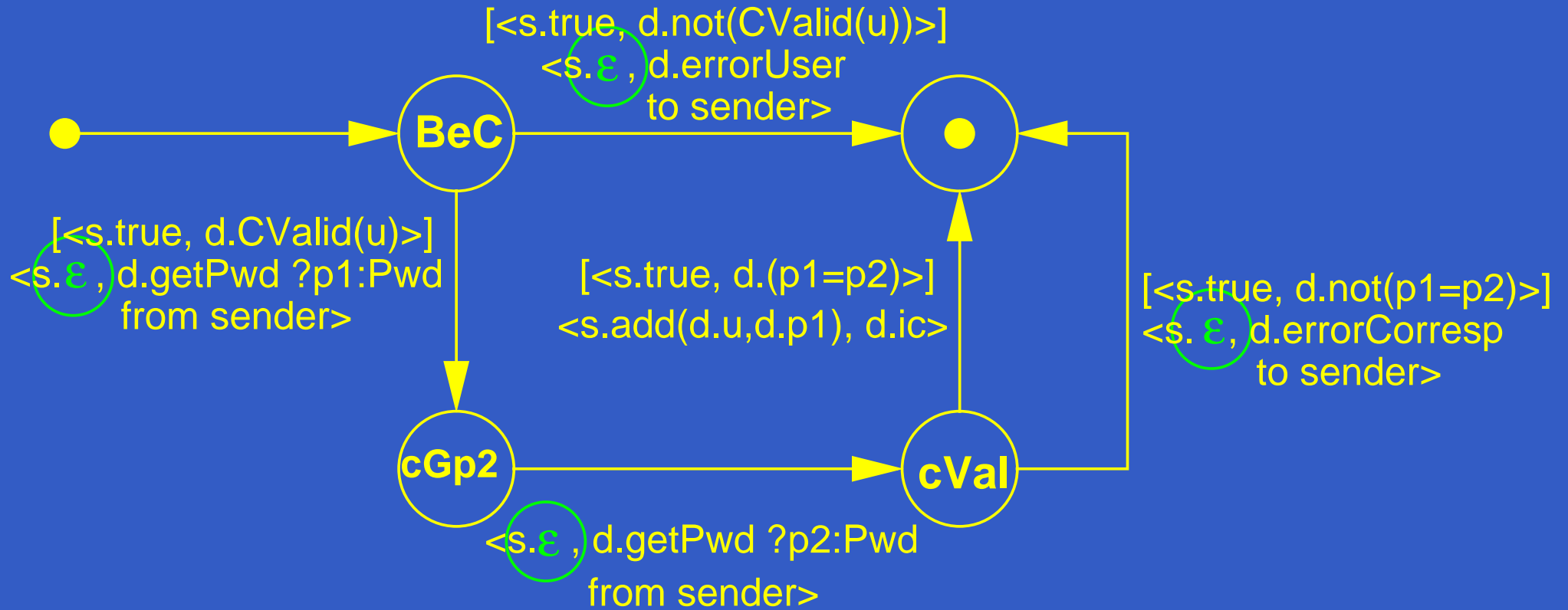
Le gestionnaire de mots de passe (STS global)



Le gestionnaire de mots de passe (STS global)



Le gestionnaire de mots de passe (STS global)



Sémantique opérationnelle d'une vue globale

Sémantique opérationnelle d'une vue globale

donnée en termes :

- d'états globaux initiaux
- d'évolutions de l'état global courant

Sémantique opérationnelle d'une vue globale

donnée en termes :

- d'états globaux initiaux
- d'évolutions de l'état global courant

un état global est représenté par :

Sémantique opérationnelle d'une vue globale

donnée en termes :

- d'états globaux initiaux
- d'évolutions de l'état global courant

un état global est représenté par :

- un état courant de la partie STS
 - un état du STS global

Sémantique opérationnelle d'une vue globale

donnée en termes :

- d'états globaux initiaux
- d'évolutions de l'état global courant

un état global est représenté par :

- un état courant de la partie STS
 - un état du STS global
- un état courant de la partie données
 - un terme

Sémantique opérationnelle d'une vue globale

donnée en termes :

- d'états globaux initiaux
- d'évolutions de l'état global courant

un état global est représenté par :

- un état courant de la partie STS
 - un état du STS global
- un état courant de la partie données
 - un terme
- un ensemble de liaison de variables

Évolution : franchissement des transitions

franchissement d'une transition contrôlé par :

- l'état global courant du STS

Évolution : franchissement des transitions

franchissement d'une transition contrôlé par :

- l'état global courant du STS
- une correspondance entre événement attendu (étiquette de la transition) et événement reçu (environnement)

Évolution : franchissement des transitions

franchissement d'une transition contrôlé par :

- l'état global courant du STS
- une correspondance entre événement attendu (étiquette de la transition) et événement reçu (environnement)
- un ensemble courant de liaisons de variables

Évolution : franchissement des transitions

franchissement d'une transition contrôlé par :

- l'état global courant du STS
- une correspondance entre événement attendu (étiquette de la transition) et événement reçu (environnement)
- un ensemble courant de liaisons de variables
- la valeur courante d'un terme représentant les données

Évolution : franchissement des transitions

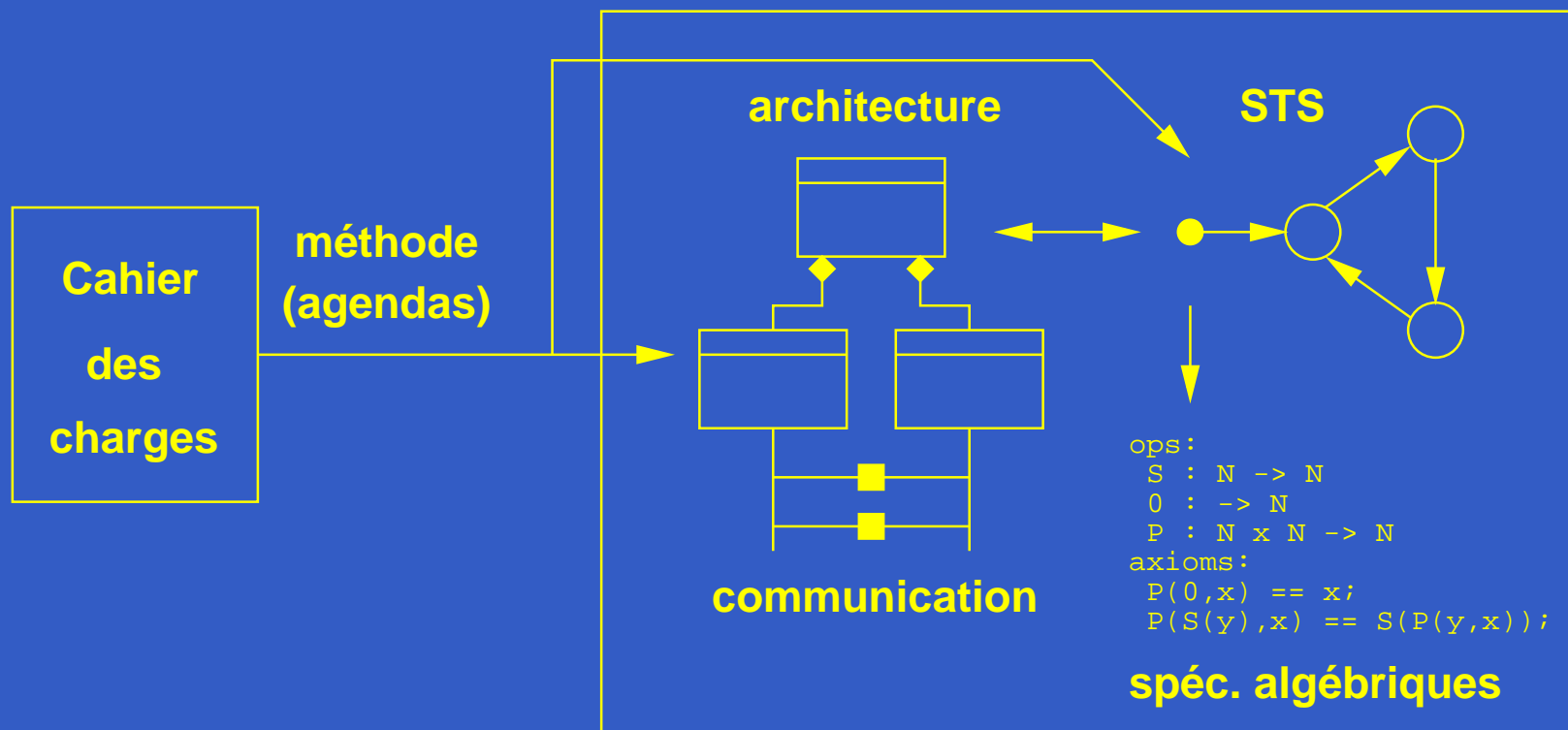
franchissement d'une transition contrôlé par :

- l'état global courant du STS
- une correspondance entre événement attendu (étiquette de la transition) et événement reçu (environnement)
- un ensemble courant de liaisons de variables
- la valeur courante d'un terme représentant les données
- des gardes évaluées dans le contexte de la partie données

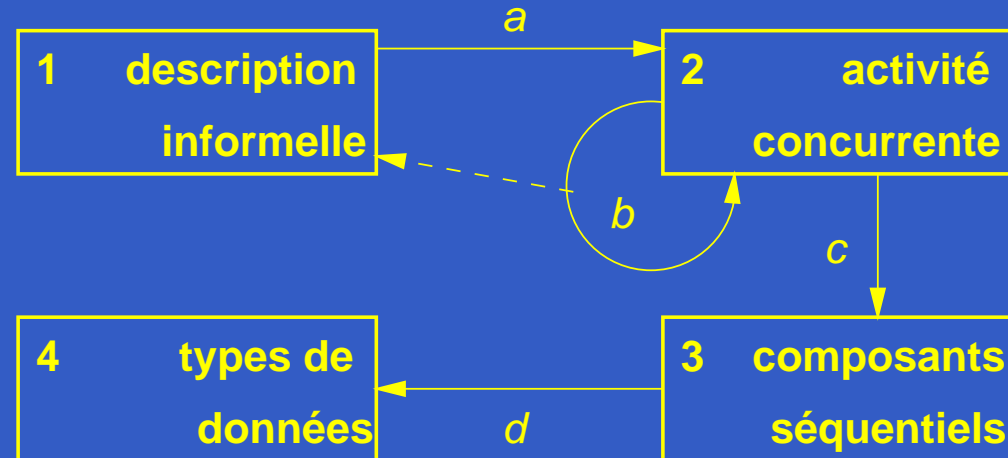
OUI, **MAIS** ...

- comment faire pour créer les spécifications ?
- je n'aime pas les spécifications formelles !
- moi, je préfère UML !

3 - Méthode de spécification pour systèmes mixtes



Une méthode en 4 étapes

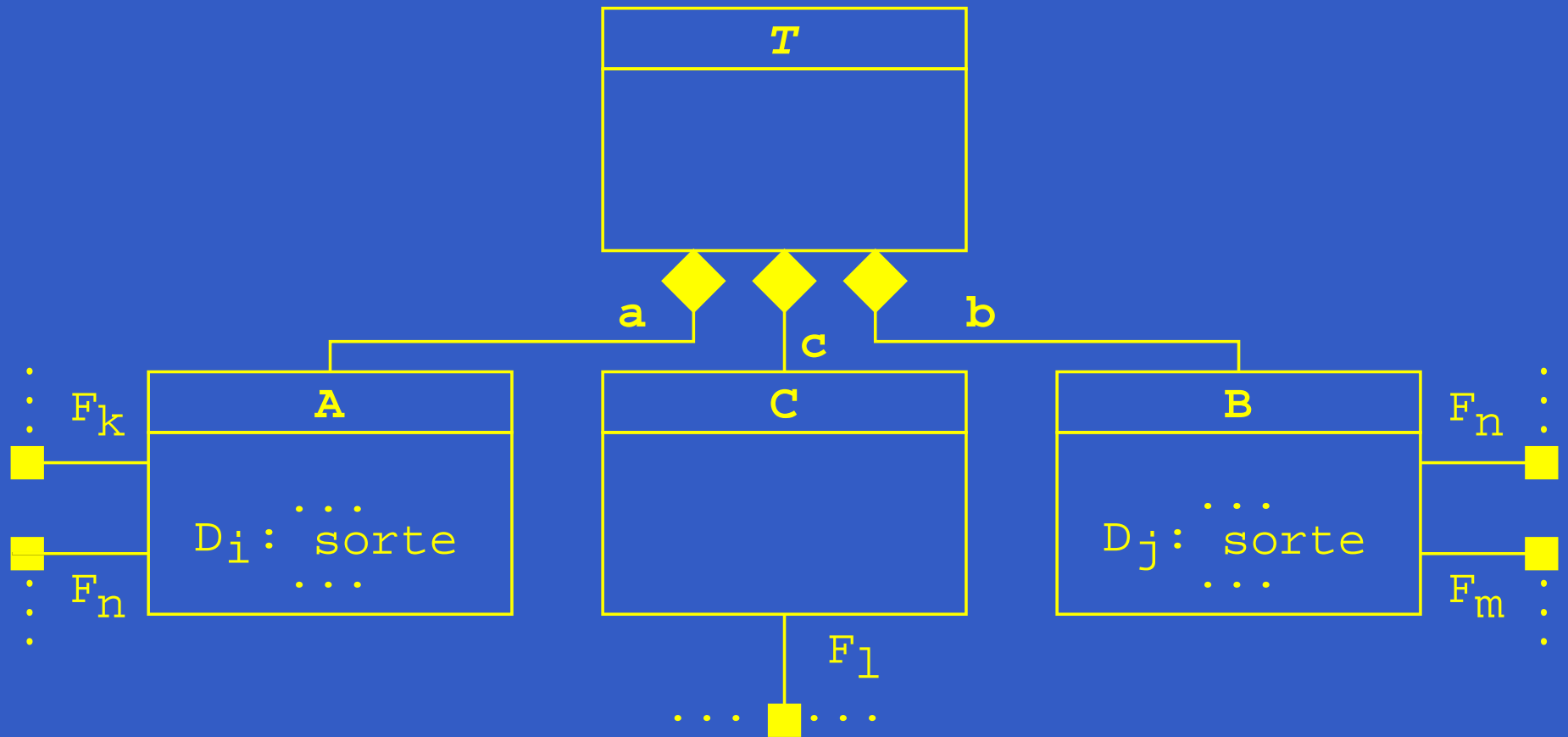


- décrite en termes d'**agendas** (semi-formelle)
- utilisation de notations graphiques, inspirées par UML
 - ➡ mais dans une approche plus orientée composants dynamiques
 - ➡ et avec un nombre plus restreint de diagrammes
- avec des aides à la spécification formelle

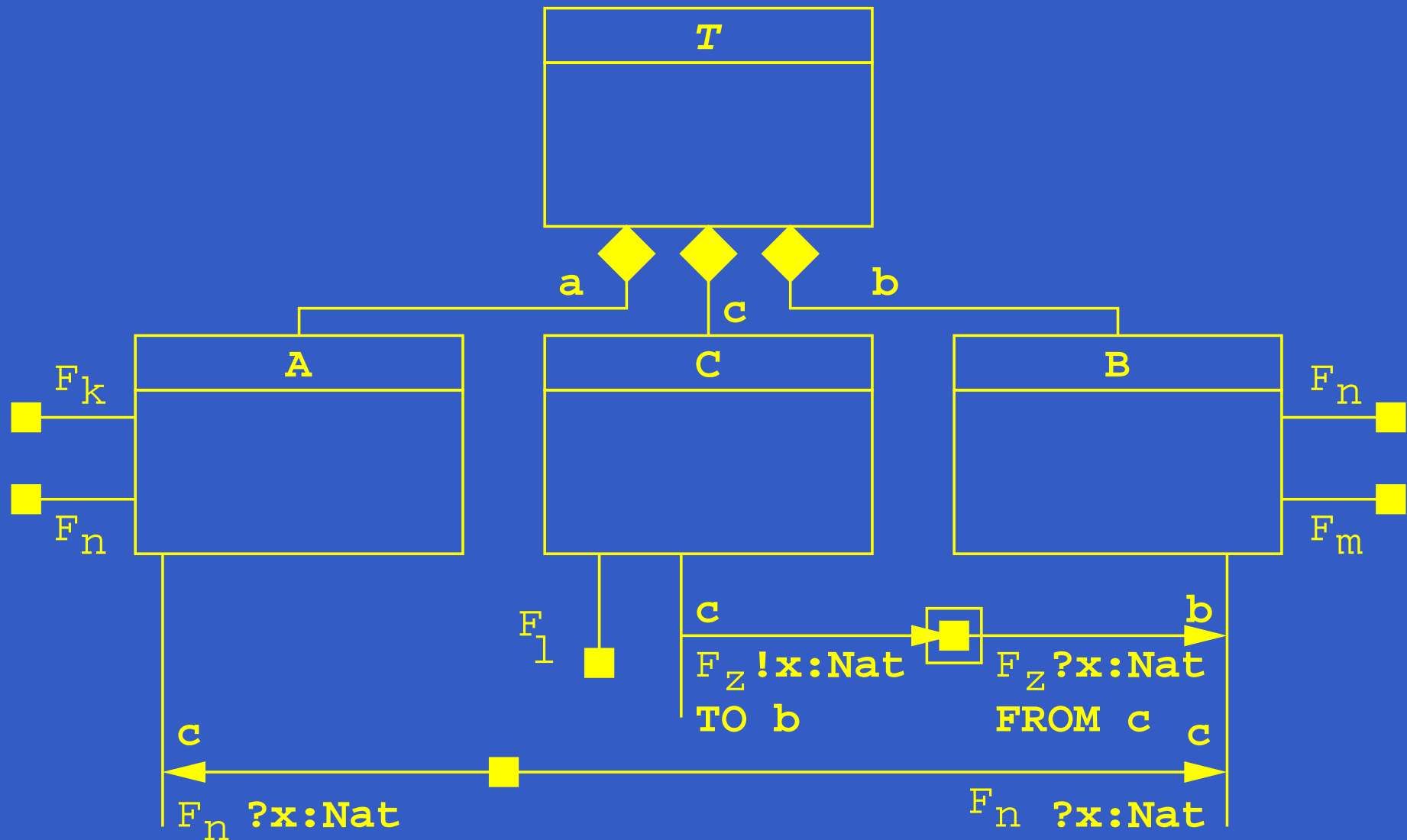
Activité concurrente : interfaces de communication



Activité concurrente : architecture



Activité concurrente : communication



Analyse des besoins

Analyse des besoins $\xrightarrow{1}$ STS

1. selon l'approche KORRIGAN :

- définition de conditions
- relations entre conditions
- valeurs initiales des conditions
- opérations définies à base de pré et postconditions

Composants séquentiels

Analyse des besoins $\xrightarrow{1}$ STS $\xrightarrow{2}$ **Spécification algébrique**

1. selon l'approche KORRIGAN :

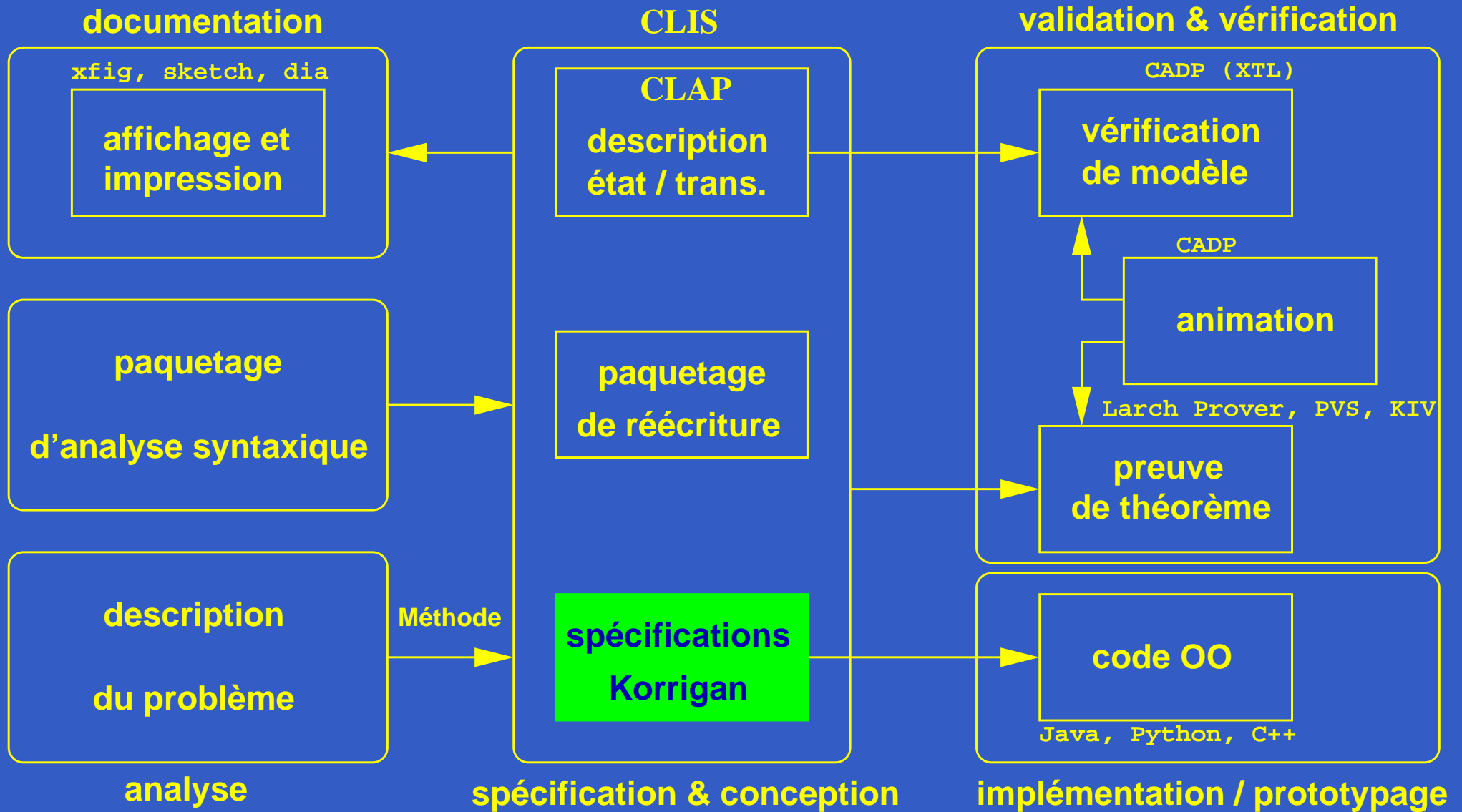
- définition de conditions
- relations entre conditions
- valeurs initiales des conditions
- opérations définies à base de pré et postconditions

2. selon l'approche (Ω -dérivation) des TAG [And95] :

- choix des générateurs relatif à l'atteignabilité des états
- dérivation des axiomes par rapport aux transitions

4 - ASK : un Atelier pour Spécifier avec KORRIGAN

Architecture



5 - Conclusions et perspectives

- formalisme et modèle [INT'2000]
sémantique : [AMAST'2000]
- méthode [WADT'98], [FASE'2001]
génération de code : [FM'99]
- atelier [J.UCS]
- perspectives

Conclusions (formalisme)

- approche hétérogène des composants (**expressivité**)
- utilisation des STS (**abstraction**)
- notations textuelles **et** graphiques (**lisibilité**)
- **structuration** des spécifications mixtes
- approche **unifiée** des aspects
- sémantique opérationnelle
- séparation des aspects, réutilisabilité
- orientation composants

Conclusions (méthode et atelier)

méthode semi-formelle pour spécifications mixtes :

- intégrant une notation inspirée d'UML
- construction semi-automatique
 - ◆ des parties comportements (STS)
 - ◆ des parties données (dérivation)

Conclusions (méthode et atelier)

méthode semi-formelle pour spécifications mixtes :

- intégrant une notation inspirée d'UML
- construction semi-automatique
 - ◆ des parties comportements (STS)
 - ◆ des parties données (dérivation)

atelier :

- implantation des mécanismes et outils du modèle et de la méthode

Conclusions (méthode et atelier)

méthode semi-formelle pour spécifications mixtes :

- intégrant une notation inspirée d'UML
- construction semi-automatique
 - ◆ des parties comportements (STS)
 - ◆ des parties données (dérivation)

atelier :

- implantation des mécanismes et outils du modèle et de la méthode **mais** dans un esprit d'ouverture

Conclusions (méthode et atelier)

méthode semi-formelle pour spécifications mixtes :

- intégrant une notation inspirée d'UML
- construction semi-automatique
 - ◆ des parties comportements (STS)
 - ◆ des parties données (dérivation)

atelier :

- implantation des mécanismes et outils du modèle et de la méthode **mais** dans un esprit d'ouverture
 - mécanismes et outils génériques
 - traductions (génération de code, vérification)

- moyens de vérification et de validation améliorés
 - ➡ traduction vers des formalismes homogènes
 - ➡ vérification de modèle + solveur de contraintes
- amélioration du niveau d'abstraction
- améliorations de la **méthode**
 - ➡ interface graphique (projet de DUT)
 - ➡ environnements dédiés méthode
 - ➡ mécanismes d'aide à la réutilisation
 - ➡ utilisation de l'aspect orienté composant du modèle dans le cadre de la programmation par aspects (sujet DEA)

- améliorations de l'atelier
 - interface graphique (projet de DESS)
 - portage d'outils
 - extension de la génération de code

FIN

KORRIGAN [kɔʁiɡã̃n] n. Myth. ; du breton *korrig* (lutin), et *gan* (chanter). ♦ Lutin chantant des légendes bretonnes, tantôt bienveillant, tantôt malveillant. ⇒ **lutin, nain.**