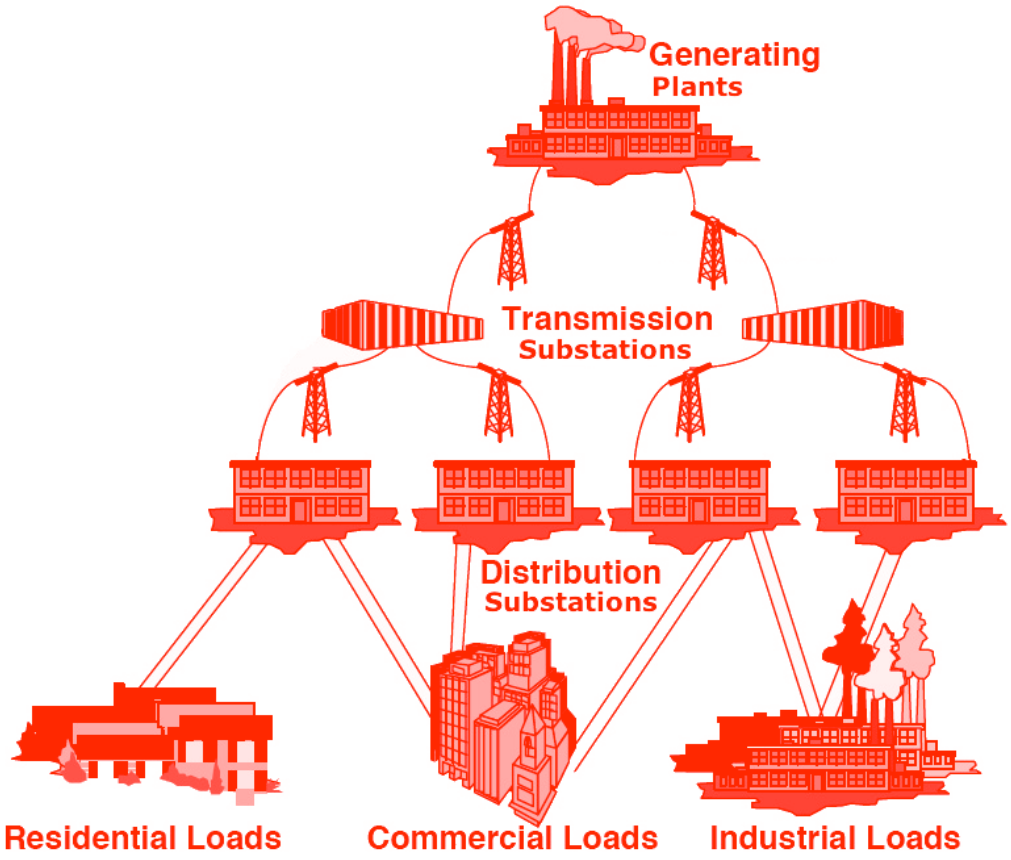
Contrôle d'accès pour les systèmes collaboratifs : une approche basée Services Web

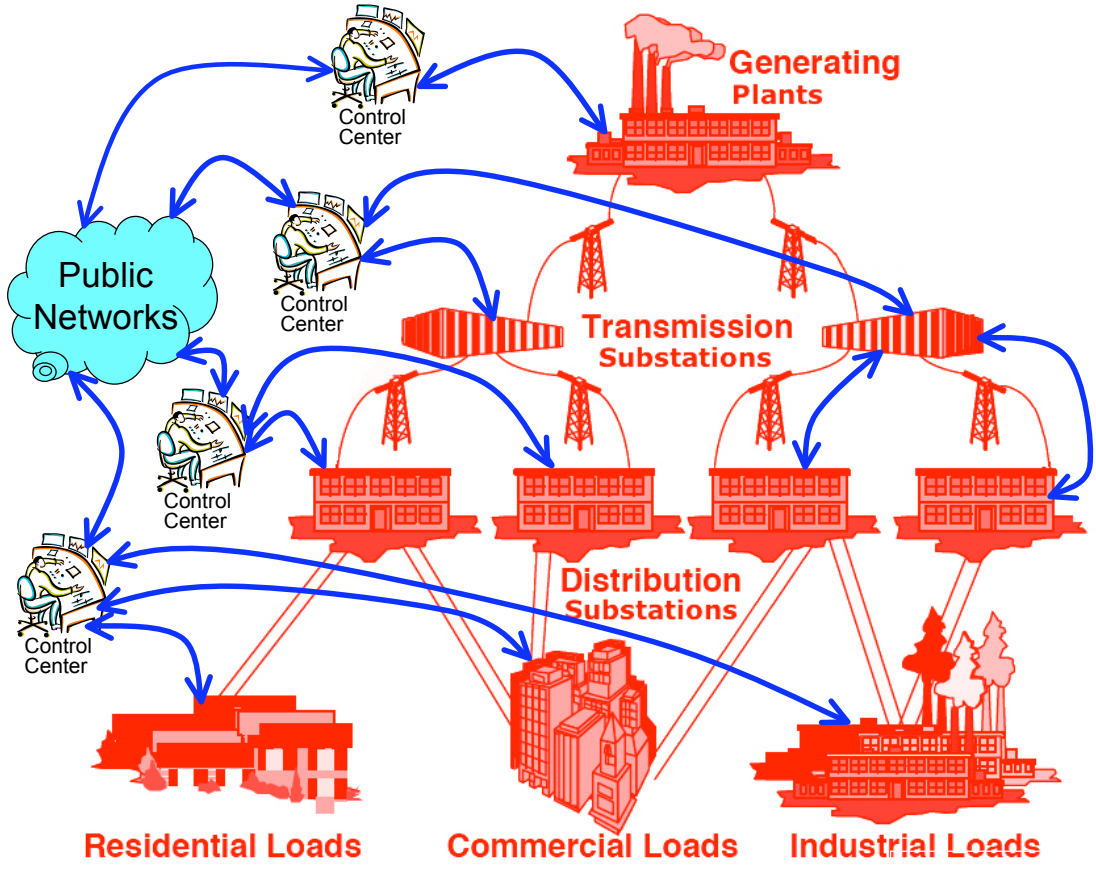
Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, Toulouse, France

Exemple d'infrastructure critique

- Production, transport, distribution d'énergie électrique en Europe : projet CRUTIAL
  - Infrastructure éléctrique
  - Infrastructure du système d'information (qui contrôle l'infrastructure électrique)


Generating
Plants
Transmission
Substations
Distribution
Substations
Residential Loads
Commercial Loads
Industrial Loads


Control
Center
Generating
Plants
Public
Networks
Control
Center
Transmission
Substations
Control
Center
Control
Center
Distribution
Substations
Residential Loads
Commercial Loads
Industrial Loads

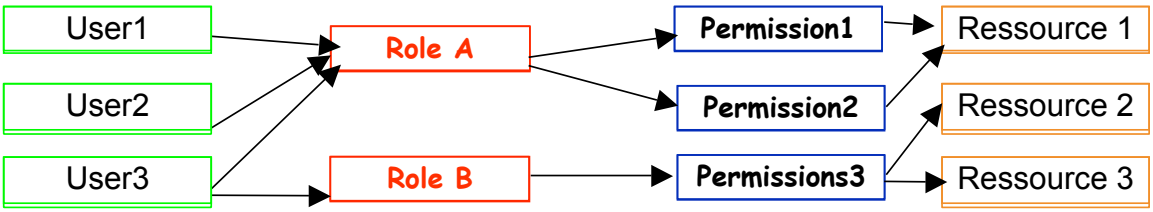
European Electrical Power Grid

- Nombreuses parties prenantes, de toutes tailles (de multinationales à TPME et particuliers), avec des fonctions variées (production, transport, distribution, commercialisation, courtage, autorités de régulation, …)
- Large étendue géographique, sur plusieurs pays
- Système d'information :
  hétérogène, complexe, dynamique, flexible
- Nécessité de coopération malgré concurrence/méfiance
  - Interopérabilité
  - Indépendance et autonomie

Modèles de sécurité pour systèmes collaboratifs

- RBAC
- OrBAC
- PolyOrBAC

RBAC: *Role Based Access Control*



- Les rôles correspondent aux fonctions dans l'organisation : facile à comprendre et à administrer
- …dans la vision d'une autorité unique !

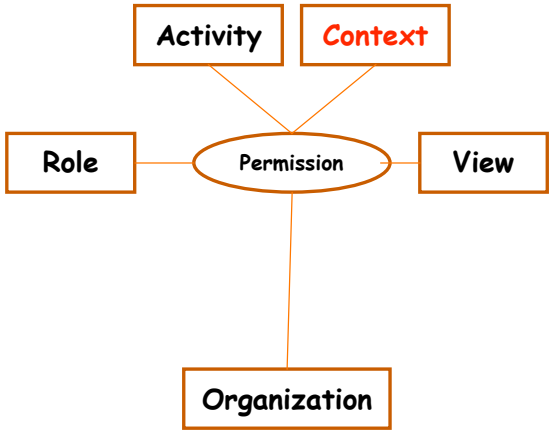
Application aux IC ?

- 1ère approche : autonomie :
  - Les utilisateurs d'une organisation (1) doivent obtenir des permissions valables dans une autre (2)
  - Liaisons users (1) -> rôle ? + rôle ? -> permission (2)
  - Responsabilité ?
  - Cohérence ?
  - Si N organisations, complexité % NxN
- 2ème approche : super-organisation
  - Imposer une politique de sécurité commune à toutes les organisations, authentification de tous les users, gestion de toutes les ressources
  - Si N organisations, complexité % (u,r,o,a)xN

OrBAC : Organization-based AC

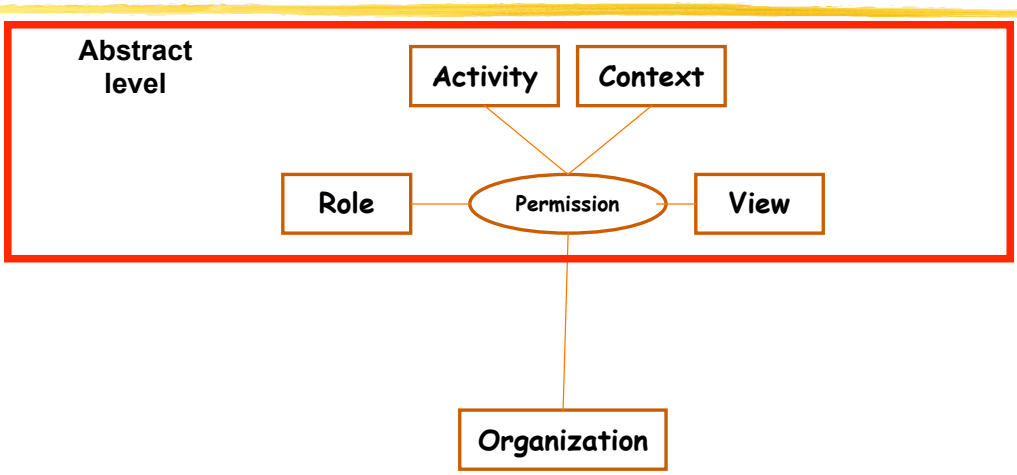
- Abstractions :
  - User -> rôle
  - Objet -> vue
  - Action -> activité
- Liaisons entre niveaux abstrait (*politique*) & concret (*mécanismes de contrôle d'accès*) : définies par l'organisation
- Règles :
  - Définies au niveau abstrait
  - Permissions/interdictions + obligations
  - Validées par le contexte (concret)

OrBAC : Organization-based AC



- Politique : règles définies au niveau abstrait :
  - Permission (Organization, Role, Activity, View, B(context))
  - Interdiction (Organization, Role, Activity, View, B(context))
  - Obligation (Organization, Role, Activity, View, B(context))

OrBAC : Organization-based AC

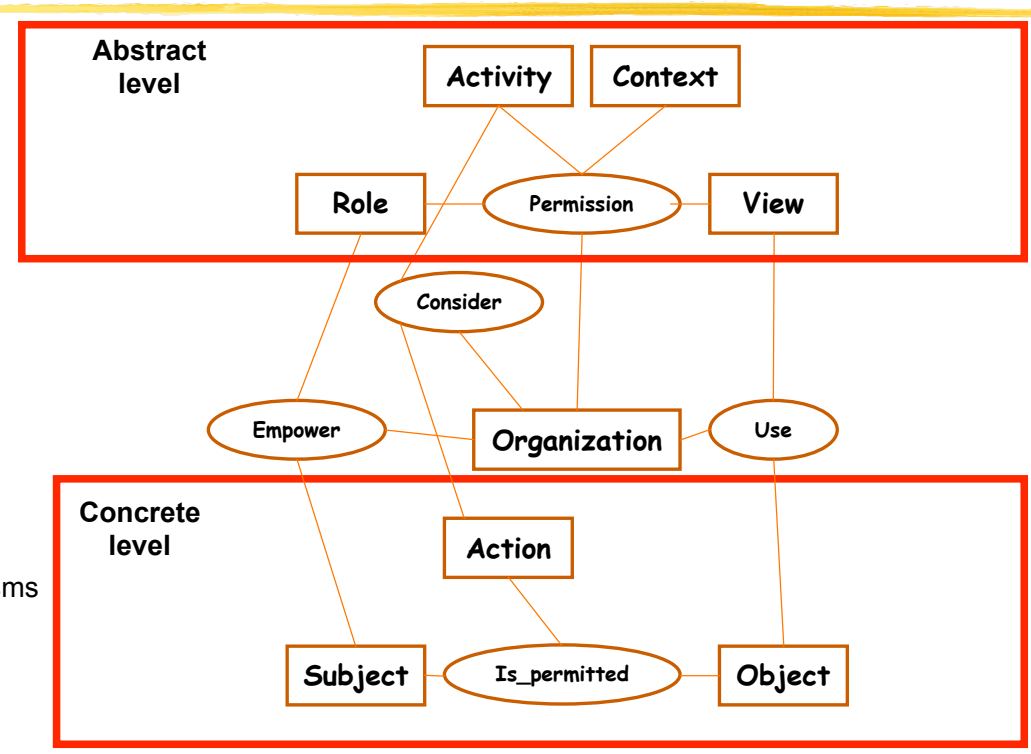


La politique est définie au niveau abstrait

OrBAC : Organization-based AC

Policy

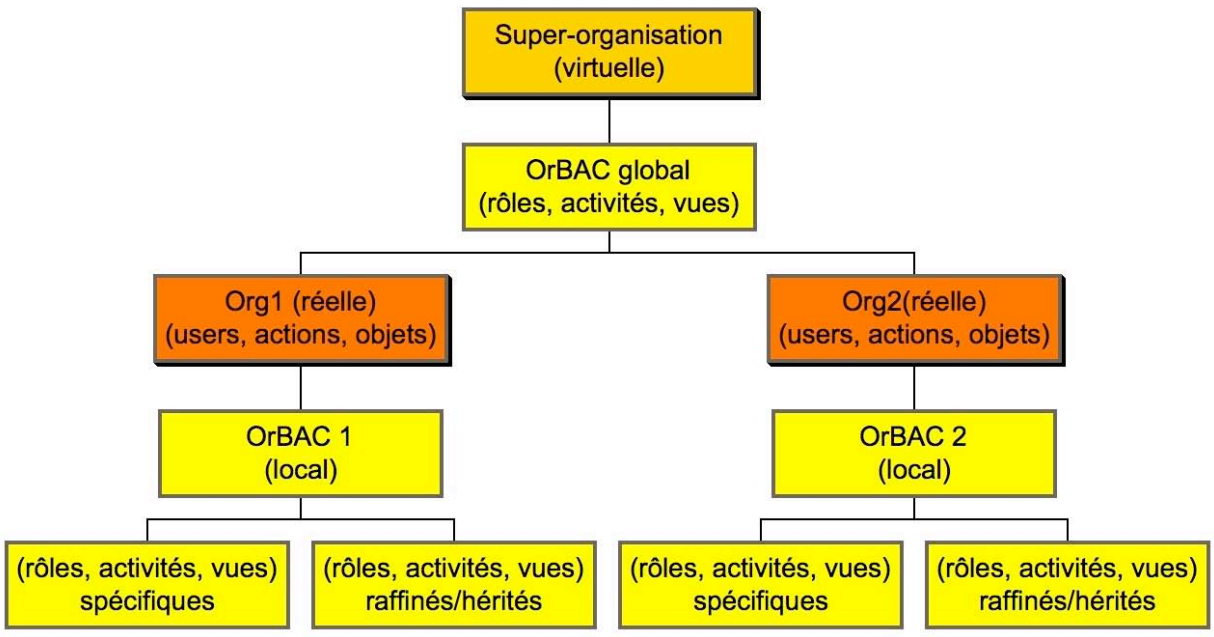
AC mechanisms



Application aux IC ?

- Mêmes approches que pour RBAC ?
  - Autonomie :
    - Qui définit les règles communes ?
    - Qui définit les liaisons abstrait/concret ?
  - Super-organisation (facilitée par la hiérarchisation dans OrBAC avec héritage)
    - Politique de sécurité commune, mais pouvant être raffinée par chaque sous-organisation
    - Complexité << NxN, mais flexibilité ?

Super-Organisation

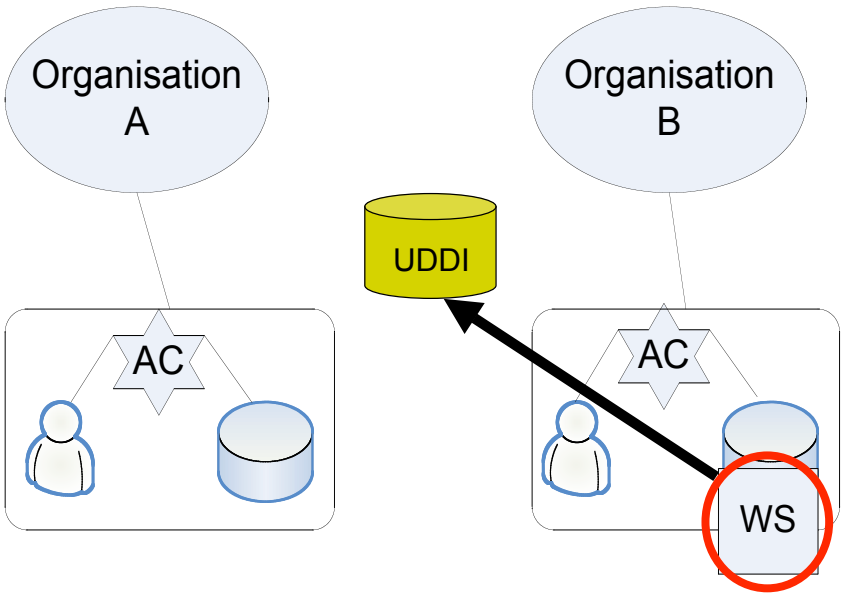


PolyOrBAC

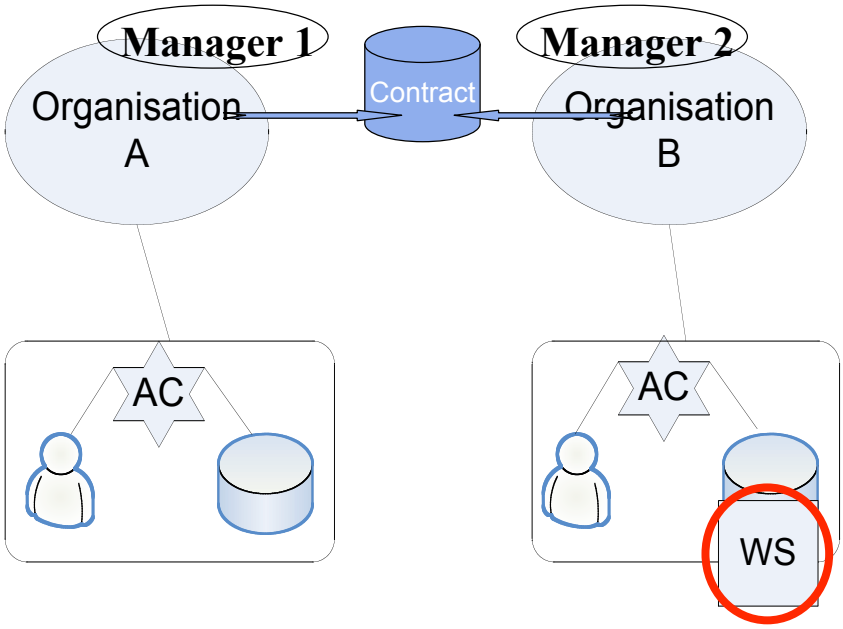
- Autonomie de chaque organisation (une politique OrBAC par organisation)

- Interaction entre organisations :
  - par Web Services : fournisseur/client
    - OrBAC du fournisseur : le WS est une activité interne, avec rôle(s) ayant permission/obligation d'exécuter le WS
    - OrBAC du client : l'appel au WS est une activité (externe), exécutable par certains rôles locaux

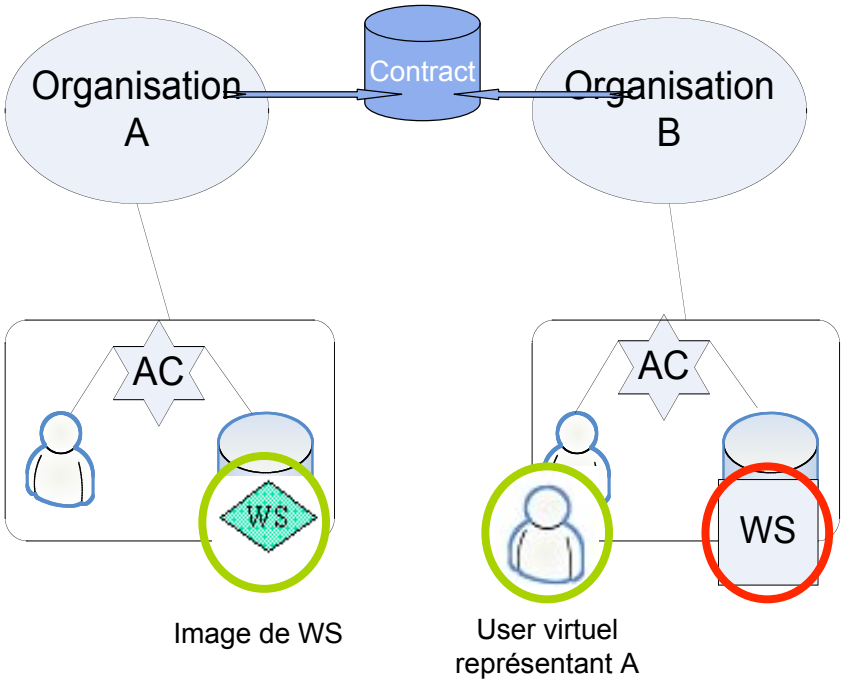
PolyOrBAC & WS



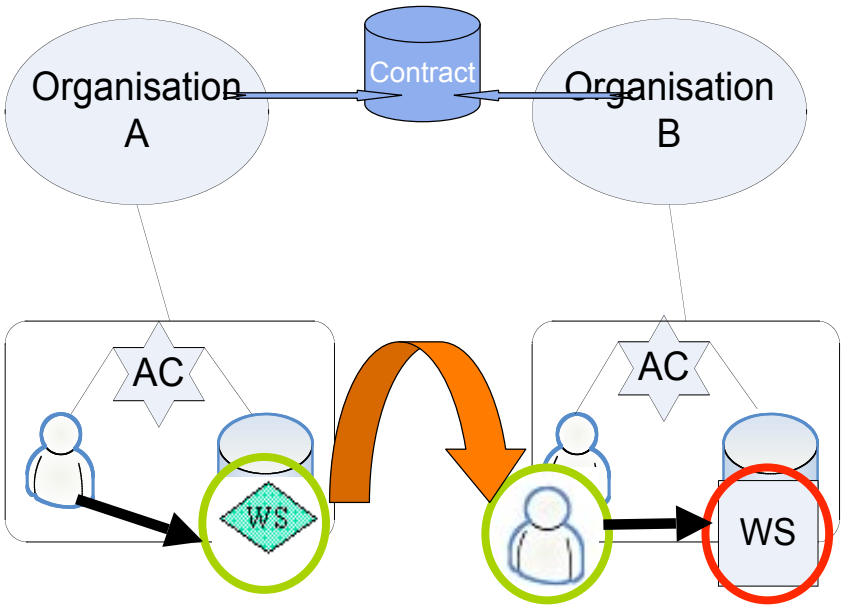
PolyOrBAC & WS



PolyOrBAC & WS



PolyOrBAC & WS

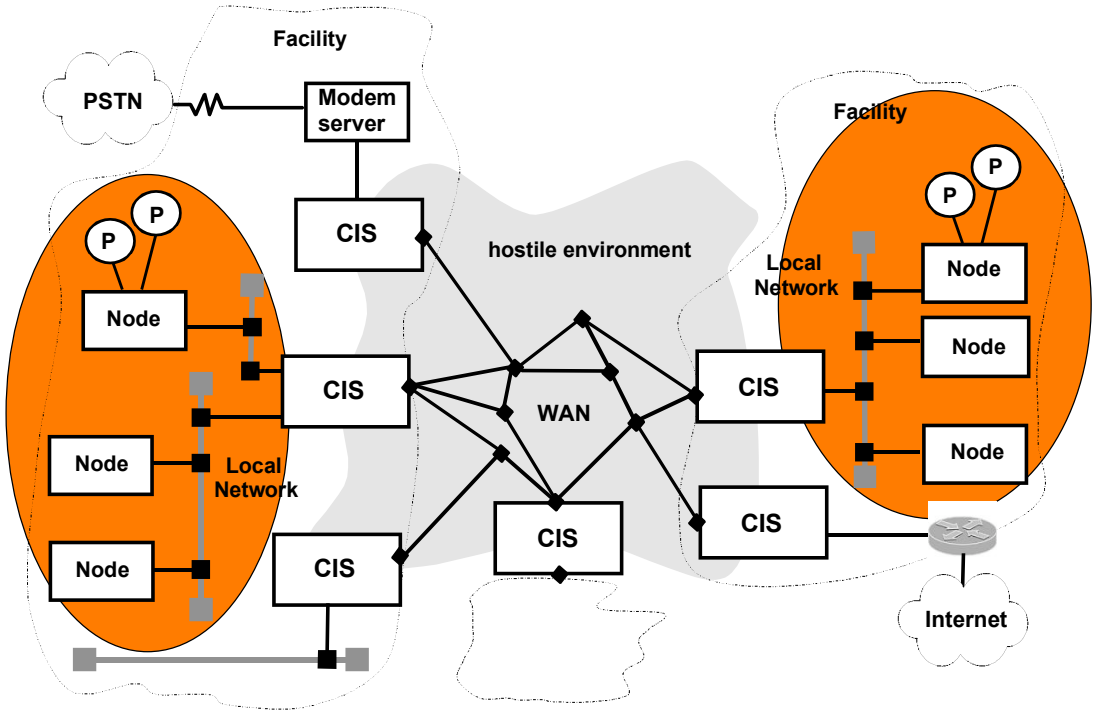


Résumé sur PolyOrBAC

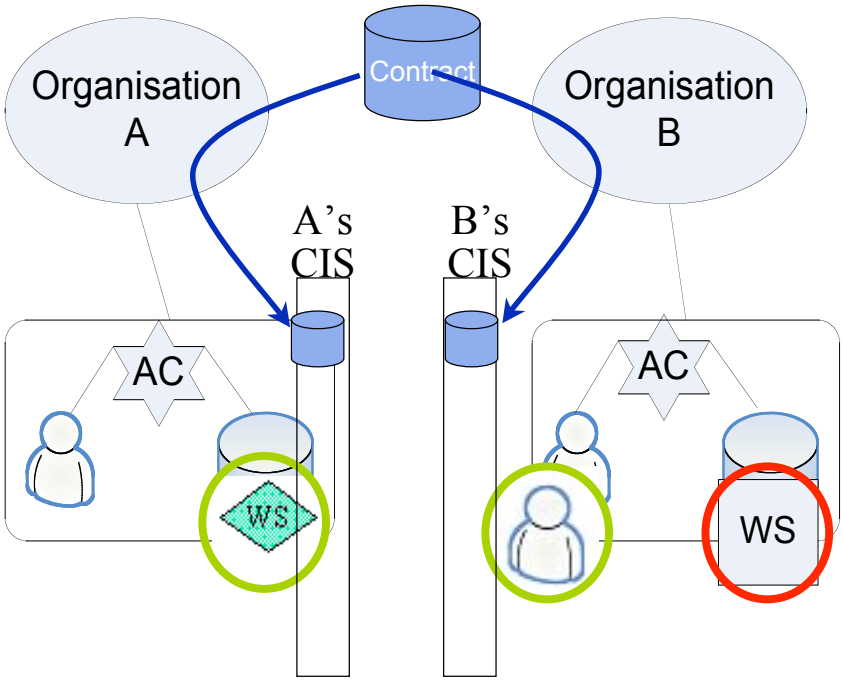
- Chaque organisation authentifie ses utilisateurs et gère ses ressources de façon autonome (politique de sécurité).

- Interactions :
  - Par Web Services, avec signature de contrats et log des échanges (preuve)
  - L'organisation cliente est responsable des actions de ses utilisateurs
  - L'organisation fournisseur est tenue de fournir le service selon les termes du contrat

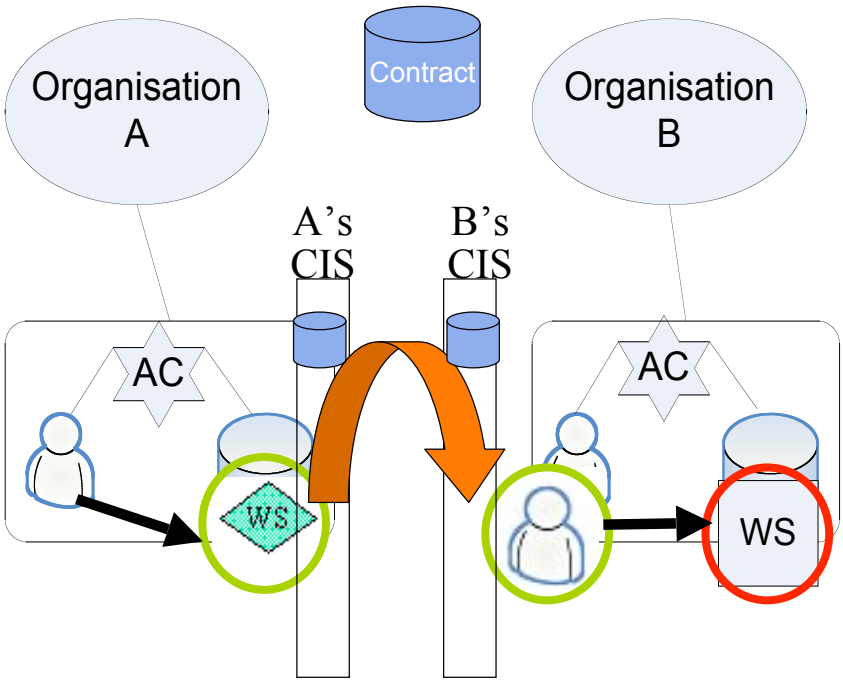
Architecture CRUTIAL



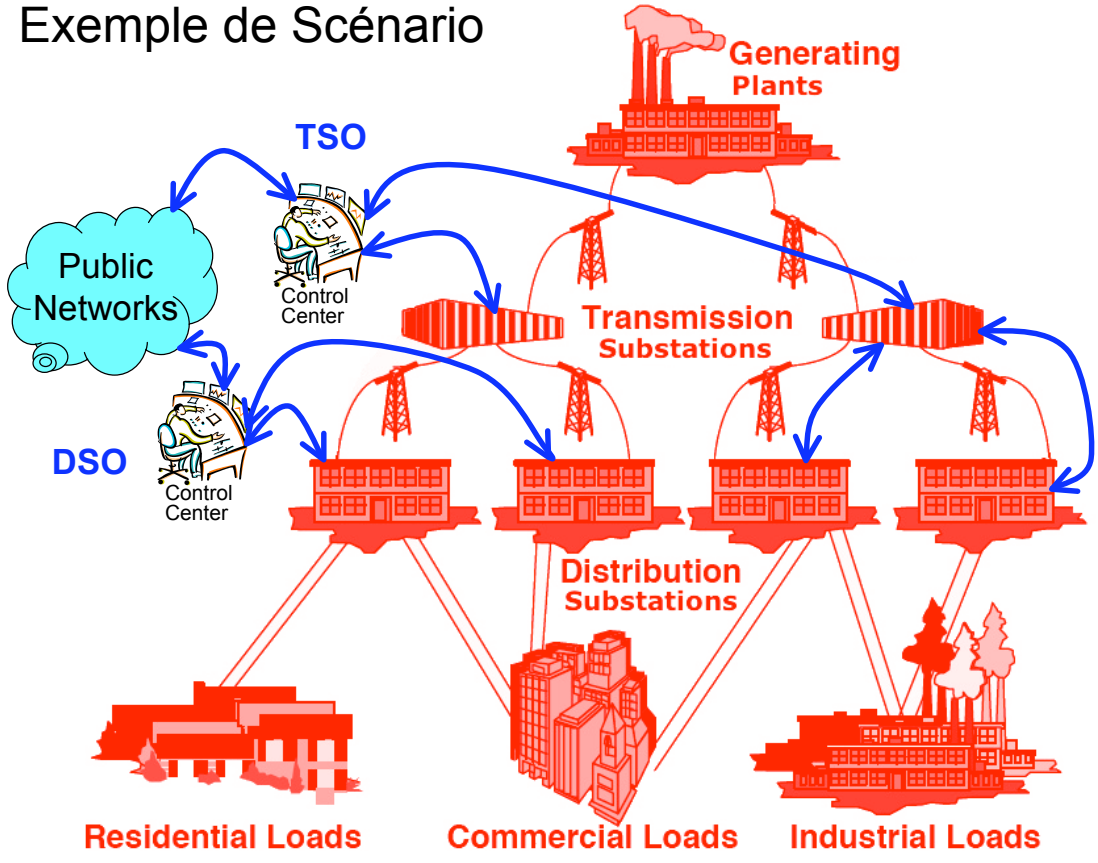
PolyOrBAC dans CRUTIAL

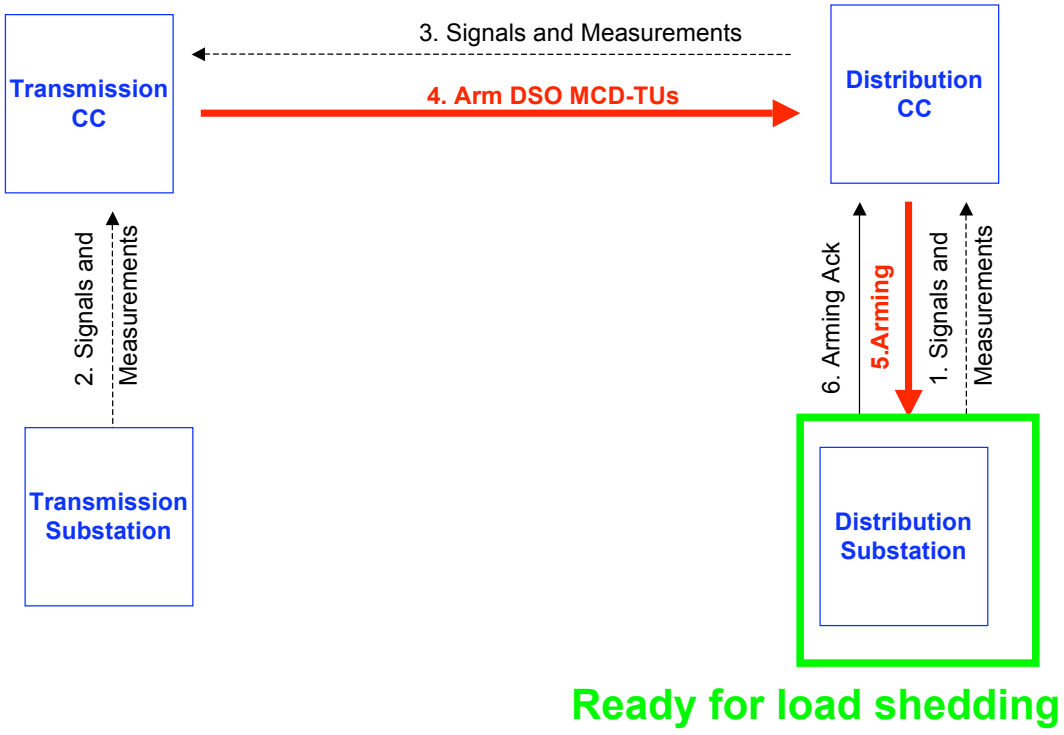


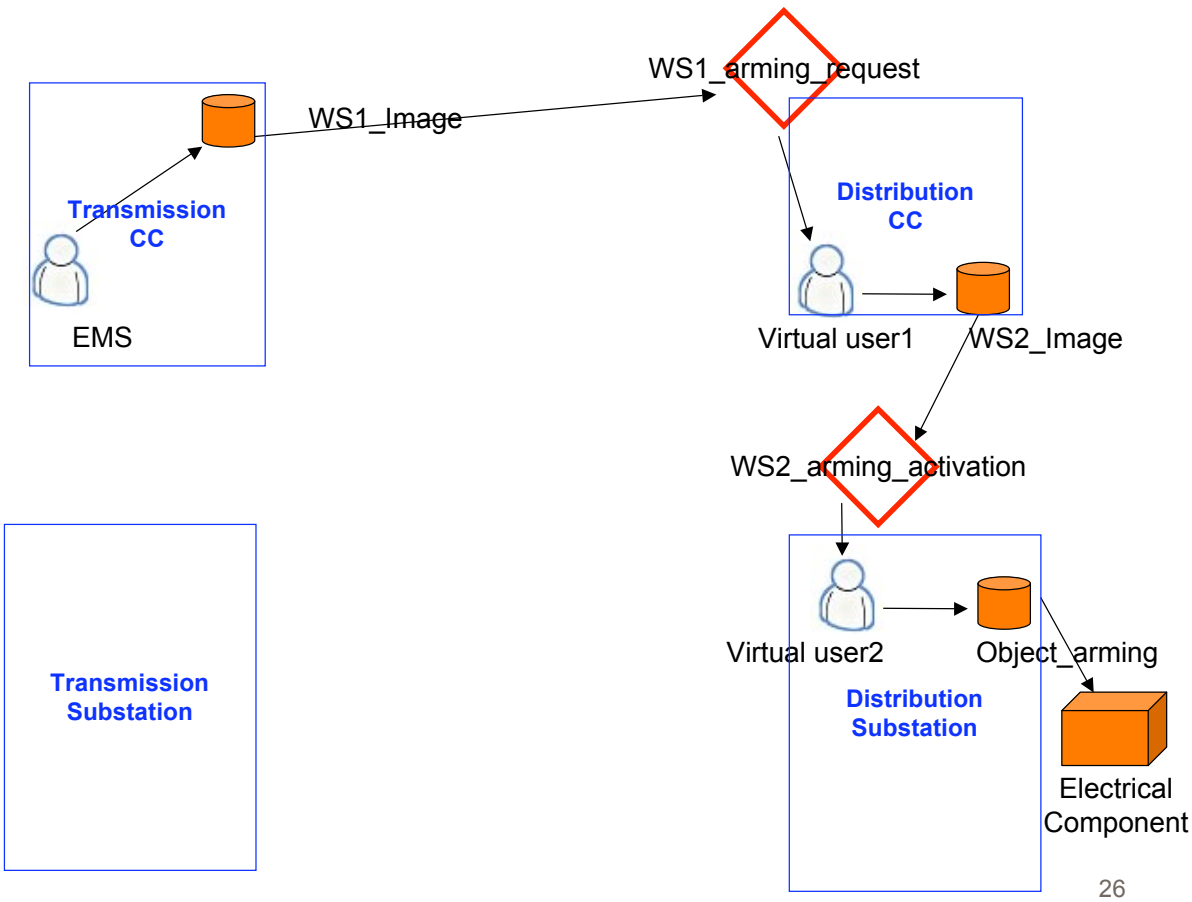
PolyOrBAC dans CRUTIAL

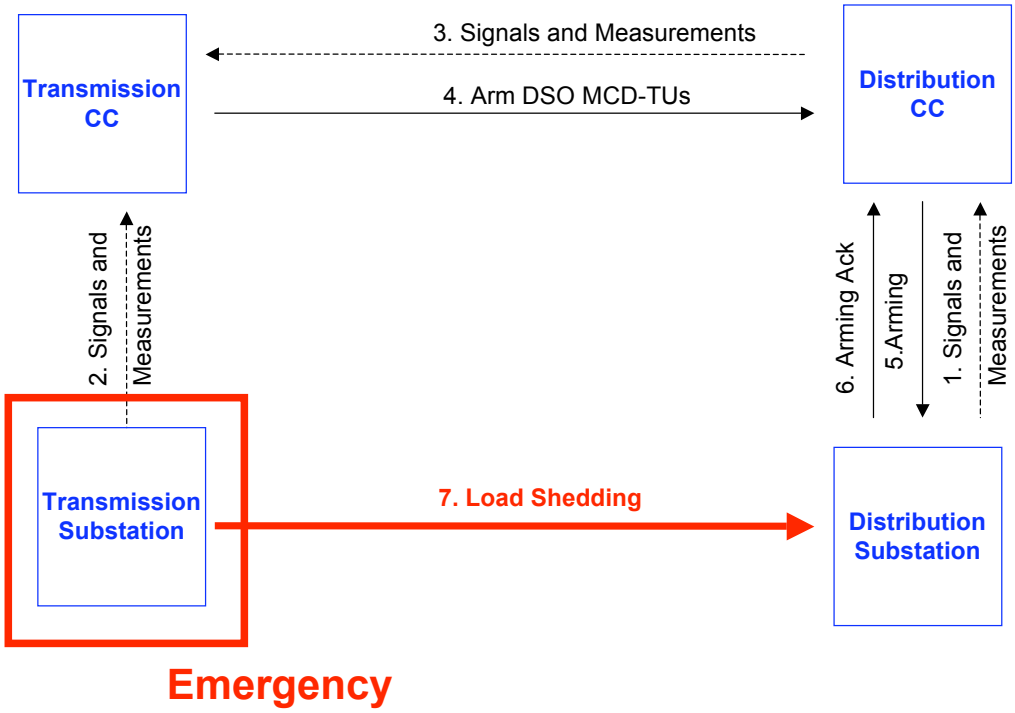


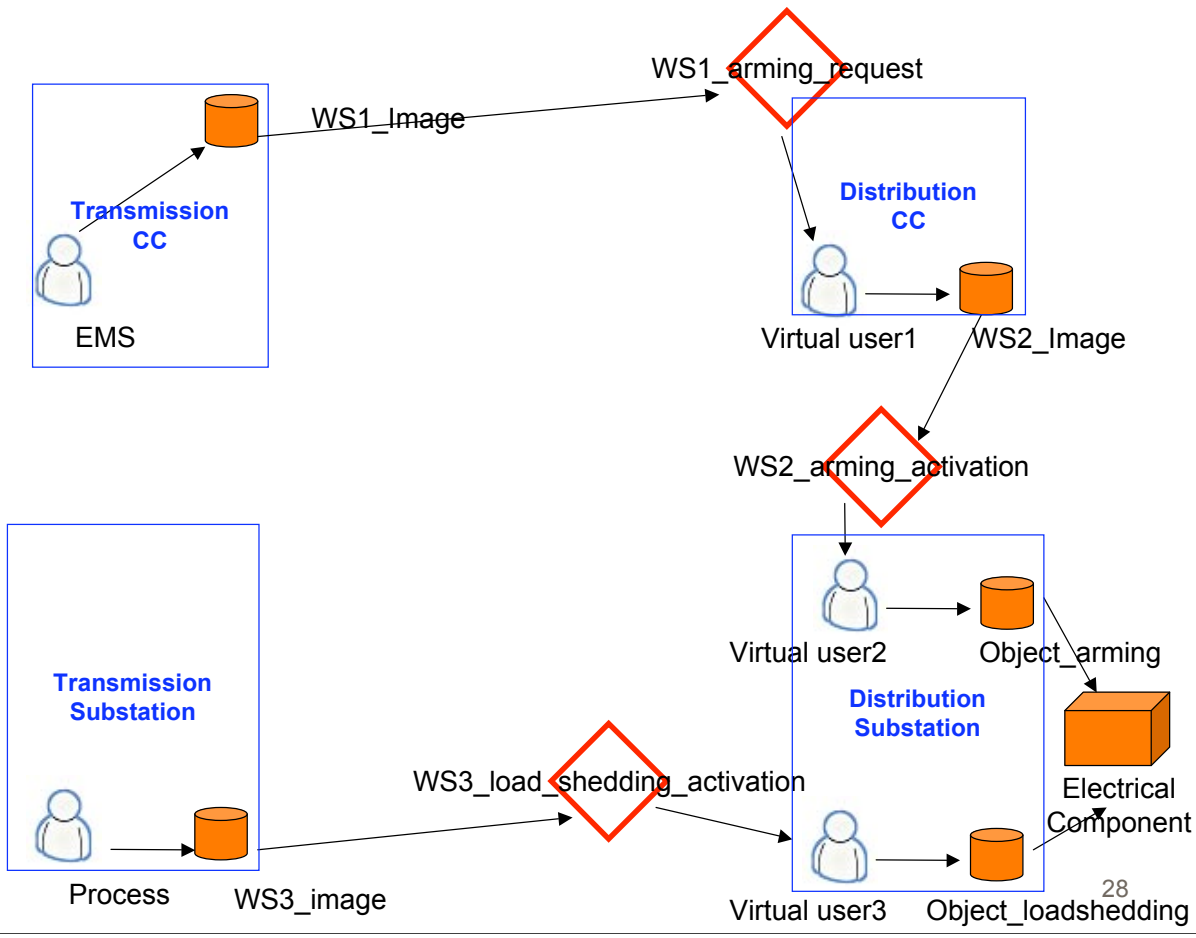
Exemple de Scénario




Transmission CC
3. Signals and Measurements
4. Arm DSO MCD-TUs
Distribution CC
2. Signals and Measurements
6. Arming Ack
5.Arming
1. Signals and Measurements
Transmission Substation
Distribution Substation
Ready for load shedding


WS1_arming_request
WS1_Image
Transmission CC
EMS
Distribution CC
Virtual user1
WS2_Image
WS2_arming_activation
Transmission Substation
Virtual user2
Object_arming
Distribution Substation
Electrical Component


Transmission CC
3. Signals and Measurements
4. Arm DSO MCD-TUs
Distribution CC
2. Signals and Measurements
6. Arming Ack
5.Arming
1. Signals and Measurements
Transmission Substation
7. Load Shedding
Distribution Substation
Emergency


WS1_arming_request
WS1_Image
Transmission CC
EMS
Distribution CC
Virtual user1
WS2_Image
WS2_arming_activation
Virtual user2
Object_arming
Distribution Substation
Electrical Component
Transmission Substation
WS3_load_shedding_activation
Process
WS3_image
Virtual user3
Object_loadshedding

Bibliographie

Anas Abou El Kalam, Yves Deswarte, Amine Baina, Mohamed Kaâniche, « Access Control for Collaborative Systems: a Web Services Based Approach », in *International Conference on Web Services* (ICWS 2007), IEEE Computer Society Press, Salt Lake City (UT, USA), 9-13 juillet 2007, pp. 1064-1071
http://ieeexplore.ieee.org/iel5/4279552/4279553/04279707.pdf?tp=&arnumber=4279707&isnumber=4279553