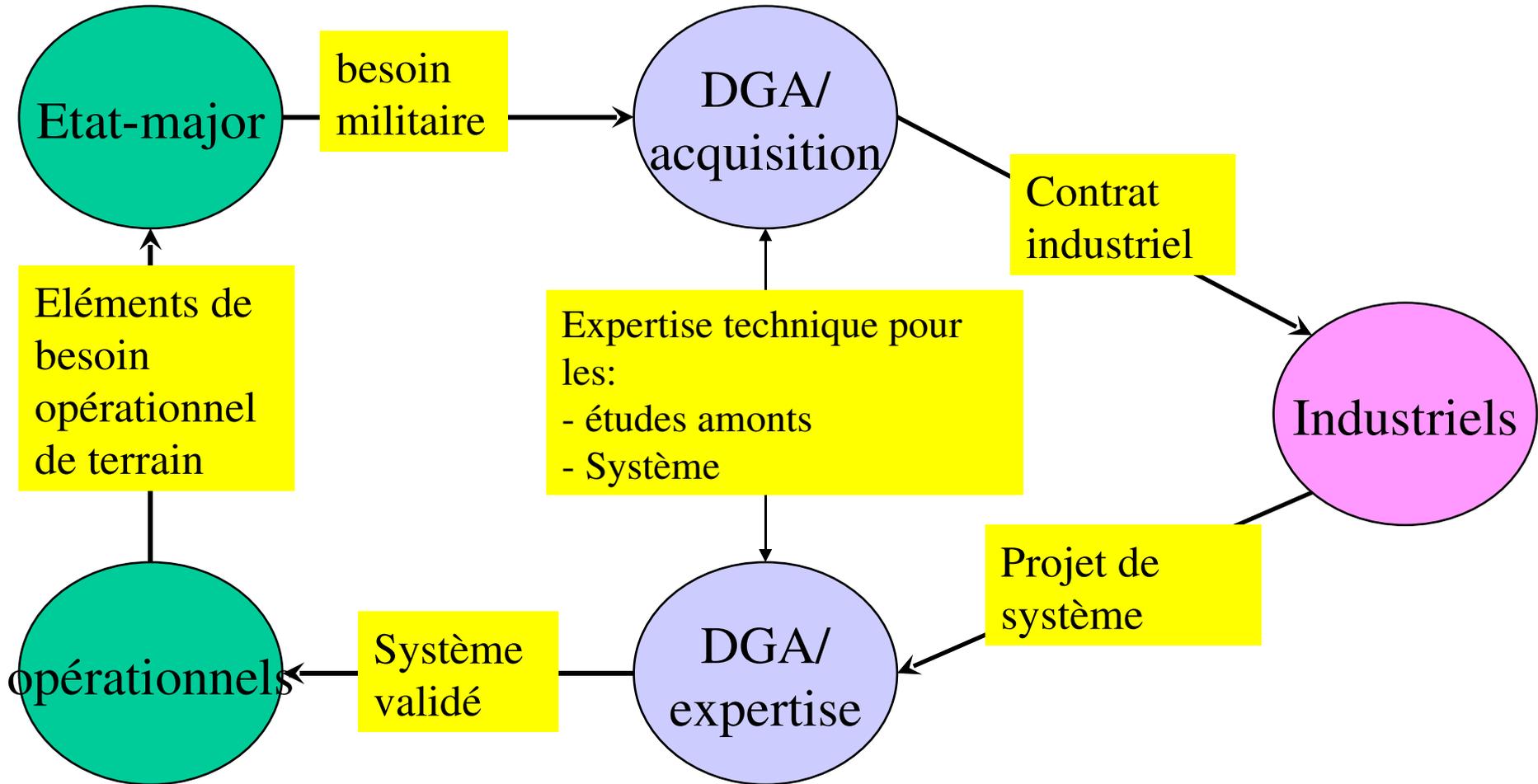


Rencontre DGA - INRIA

Quelques éléments issus du besoin opérationnel
militaire et de sécurité globale

ICETA PARRIEL André
Chef de la division SSI du CELAR

Rappel de la démarche d'ensemble d'acquisition des systèmes de défense





Quelques points majeurs du besoin opérationnel

- Une évolution vers l'emploi des technologies de l'information pour le commandement sur l'espace de bataille (infra et tactique):
 - De nombreux systèmes à connecter
 - Des métiers « humains » et très traditionnels à relier par l'informatique
- Exemple : espace de bataille terrestre, fédération des systèmes d'information pour le commandement interarmées
- Problèmes :
 - Interopérabilité des systèmes d'information
 - Gestion de la complexité des aspects transverses
 - Gestion de la sécurité
 - Explosion des besoins en volume de matériels nécessaires
 - Impossibilité de gestion statiques des flux d'information => vers des systèmes auto-organisant



Quelques points majeurs du besoin opérationnel

- Une évolution de l'analogique vers le numérique pour les systèmes de communication cibles des actions de renseignements
 - Hier : flux analogiques, pas/peu multiplexés, protocoles et services associés de très bas niveau (phonie)
 - Aujourd'hui/demain : flux numériques, fortement multiplexés, protocoles et services associés complexes et de haut niveau
- Problème :
 - Modes opératoires anciens devenus obsolètes
 - Difficultés à identifier les flux dans le train binaire
 - Remontée aux services de haut niveau



Quelques points majeurs du besoin opérationnel

- Un besoin croissant de sécurité en général et sur certains équipements de sécurité jugés critiques pour la construction de grands systèmes de communication ou pour la sécurité des systèmes exportés
 - Hier : peu d'équipement de sécurité, complexité faible, design orienté hardware et mono-service
 - Aujourd'hui/demain : croissance du nombre d'équipements ou de fonction de sécurité, complexité croissante, place croissante du software ou des représentations abstraites de design hardware
- Problèmes :
 - Maîtrise de la sécurité des nouveaux équipements
 - Place croissante du logiciel et de son caractère difficilement prouvable quant à son fonctionnement
 - Même problématique sur les aspects VHDL des gros hardwares construits



Points techniques proposés

- Les réseaux de capteurs
 - Mise en réseau auto-organisant des systèmes d'information et des capteurs de tout type
- Sécurité multi-niveau
 - Factorisation de l'informatique de l'utilisateur dans un contexte multi-niveau de sécurité (diffusion restreinte, secret défense, secret OTAN, secret UE, ...)
- Sécurité et sûreté des implémentations
 - Développement des briques de sécurité avec une exigence de très haute fiabilité, d'intégrité et de conformité aux spécifications
- Analyse du train binaire
 - Pour permettre la constitution de nouveaux systèmes de renseignements sur la base de systèmes numériques