

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

Actuator Sensor Securing over Industrial Networks

Sécurisation matérielle de capteurs/actionneurs distribués sur des réseaux industriels

Thomas Toublanc

Laboratoire des Sciences et Techniques de l'Information de la Communication et de la Connaissance

Pôle: CACS, équipe: MOCS

Supervisor: Pascal Berruet,
Co-supervisor: Florent De Lamotte



19 juin 2018

Sommaire

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

1 Contexte

- Recherche
- Physique
- Menace
- Objectif & problématique

2 Contribution

- Description de la solution
- Flot de conception
- Démonstrateur

3 Conclusion

- Bilan
- Perspective

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

modèle

Computer Integrated
Manufacturing (CIM)

- Système $\equiv \{composants\}$
- Composants \vee opérateur \Rightarrow opérations
 - Gérer
 - Superviser
 - Contrôler
 - Agir

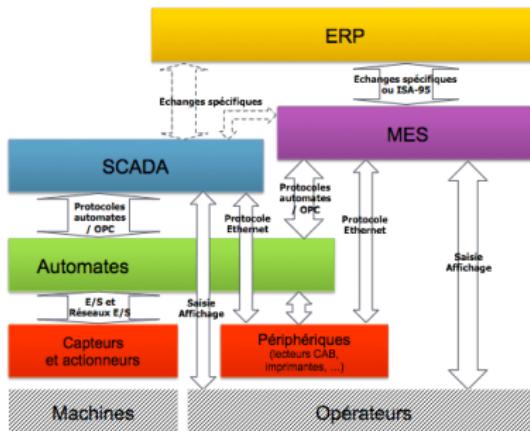


FIGURE – modèle CIM

Reference Architectural
Model Industrie 4.0 (RAMI4.0)

- Système $\equiv \{composants \vee services\} (D)$
- $D_x \Rightarrow$ $\overbrace{N_{\text{iveau}}.H_{\text{ierarchie}}, M_{\text{oment}}.V_{\text{ie}}, C_{\text{ouche}}.OP_{\text{rationnelle}}}$
- D_x communique via un shell d'administration
- $\forall D_x \exists$ interfaces(cyber \vee physique) \Rightarrow CPS

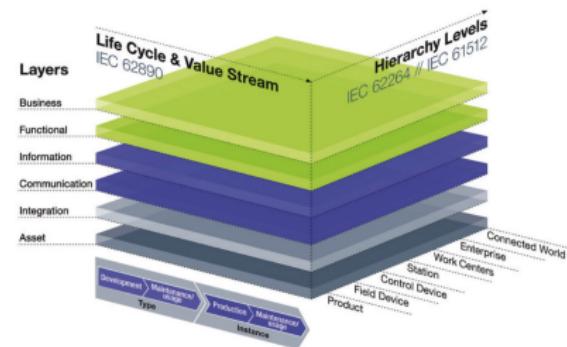


FIGURE – modèle RAMI

Décomposition par niveaux d'un système cyber-physique industriel

Intranet d'entreprise & services

- PRE = ERP(US)
- Équipement services

DMZ & supervision

- Zone démilitarisée
- Équipement supervision

Système de contrôle automatique industriel

- Automate
- Capteur & actionneur &/ IIOT (objet connecté)

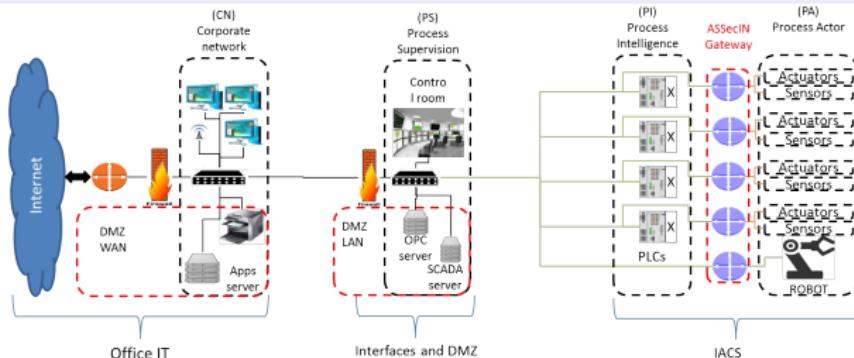


FIGURE – Représentation d'un CPS

Découverte

Les réseaux industriels sont isolés les uns des autres &/ sécurisé par niveau, mais au niveau de l'IACS il n'y a pas de sécurité sauf celles garanties par les concepteurs de solution qui sont minimes.

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

Défaillance

- Anomalie intra-système
- Causé par un/des composants ∈ système
- Ponctuelle / cyclique

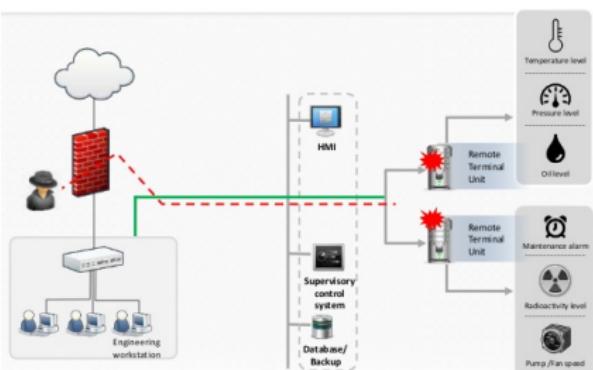


FIGURE – attaque simple [OZOOS (2015)]

Simple :

- Attaque mineure
- Attaquant ayant droit sur système
- Connaissance informatique #
- Connaissance système Δ

Attaque

- Anomalie extra-système
- Causé par une/plusieurs entité/s
- Intentionnelle & orienté

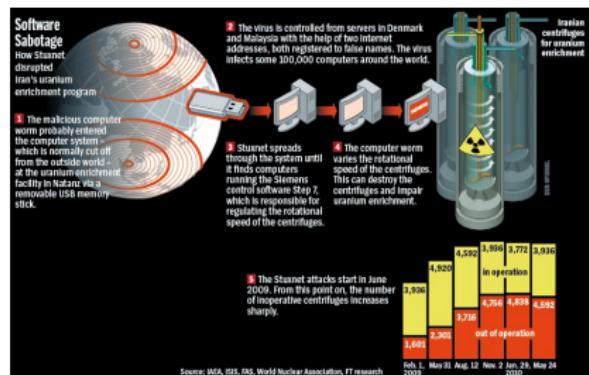


FIGURE – attaque complexe [STUXNET (2012)]

Complexe :

- Attaque majeure
- Multiples attaques en une seule
- Connaissance informatique Δ
- Connaissance système #

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

Objectif

Déetecter et réagir aux menaces sur un IACS.

Mettre en œuvre un démonstrateur avec la solution.

Problématique principale

Comment limiter l'impact des menaces sur un systèmes industriels ?

Problématique secondaire

- 1 Comment sécuriser la partie opérative d'un IACS en réseaux ?
- 2 Comment assister la configuration de la solution ?
- 3 Comment démontrer l'efficacité de la solution ?
- 4 Comment minimiser l'impact de la solution sur le système ?

ASSecIN

Thomas
Toublanc

Contexte

Recherche
Physique
Menace
Objectif &
problématique

Contribution

Description
de la
solution
Flot de
conception
Démonstrateur

Conclusion

Bilan
Perspective

Contribution : Description de la solution

Hypothèse

Proche du monde physique meilleur sont la détection et la réaction [1,4].

- Entre plusieurs réseaux → passerelle
- Passerelle Automate/PO
- Placement stratégique :
 - *Info* premier à analyser
 - **Meilleure détection**
 - *Ordres* dernier rempart
 - **Meilleure réaction**

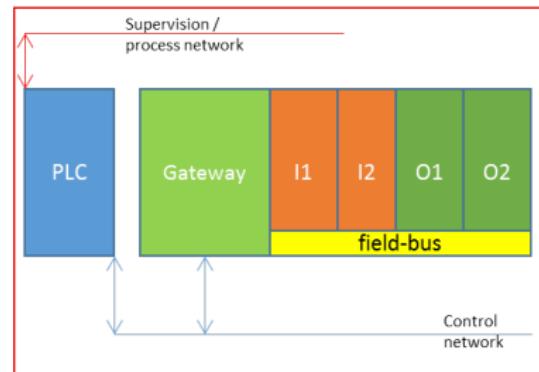


FIGURE – Placement de la passerelle

Concept

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description de la solution

Flot de conception

Démonstrateur

Conclusion

Bilan

Perspective

Hypothèse

- Déetecter & réagir s'effectuent à différentes références temporelles [1,4].
- Notre solution remonte des logs pour le SOC [1].

Concept

- 3 niveaux temporels
- Contrôle des données
- Détection & réaction

Chaines

- Communication (TL1)
- Détection (\rightarrow and \rightarrow)
- Réaction (\rightarrow)

Niveaux temporels

- 1 Syn_{chrone} avec process
- 2 Temps ordi_{nateur} async
- 3 Temps retardé pronostique anticipation

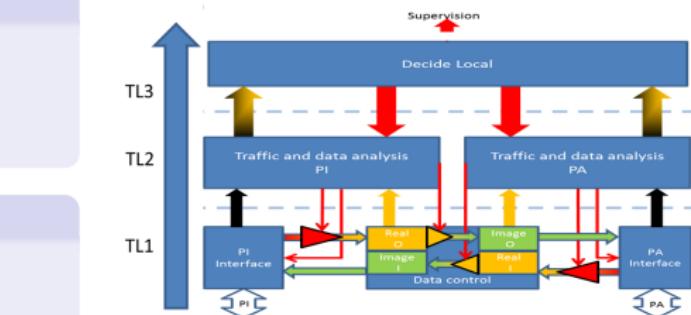


FIGURE – Concept de la passerelle

Data contrôle

- Info réseaux Réel
- Info sécurisé Image

Détection & réaction

- Direct - Réflex
- Motif - Intervalle
- Continue - Retardé

Contexte

Recherche
Physique
Menace
Objectif &
problématique

Contribution

Description
de la
solution

**Flot de
conception**

Démonstrateur

Conclusion

Bilan
Perspective

Flot de conception

Flot général

ASsecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description de la solution

Flot de conception

Démonstrateur

Conclusion

Bilan

Perspective

SimSED [Lallican(2007)]

- Partie opérative
- Code automate (bas niveaux)
- Utilisation d'une BDD composant

ComGEM [Bevan(2013)]

- Code automate (haut niveaux)
- Contrainte de commande
- Génération du code par transformation

ComSecGEM [Toublanc(2018)]

- Configuration de la passerelle
- Contrainte de sécurité
- Utilisation d'une BDD règle de sécurité
- Génération des contraintes par transformation

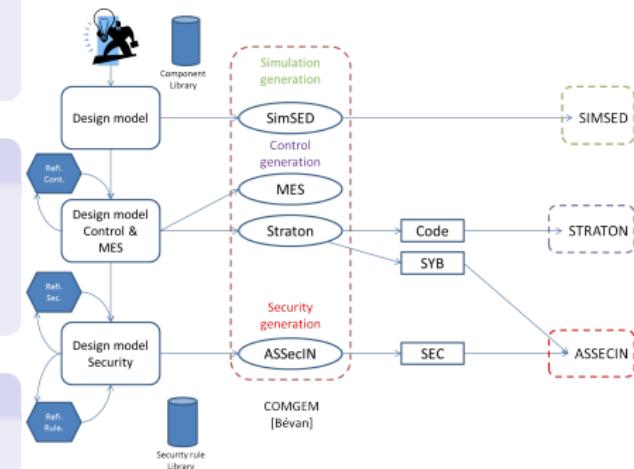


FIGURE – Flot de conception et outils

Modification Méta-modèle

Ajout de 2 vues

- Surveillance

- monitoring logique
- ordre / environnement logique

- Supervision

- réagi à la violation d'une contrainte

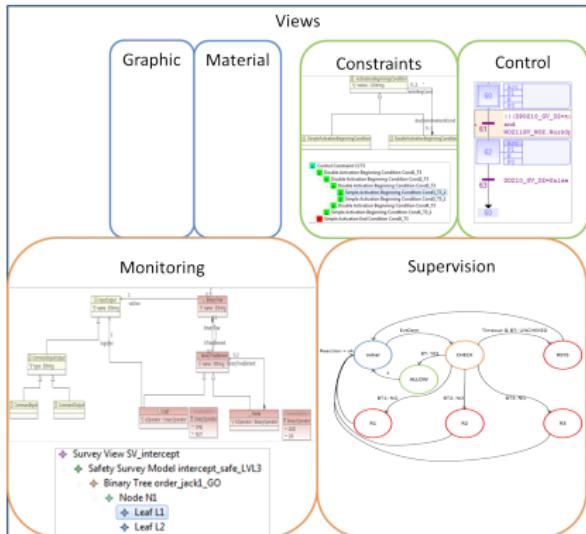


FIGURE – Présentation des vue

Transformations

- 1 génération de contrainte (surveillance - safety) par règle
- 2 modèle de conception → modèle de référence
- 3 modèle de référence → fichier de configuration XML

Flot ASSecIN

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

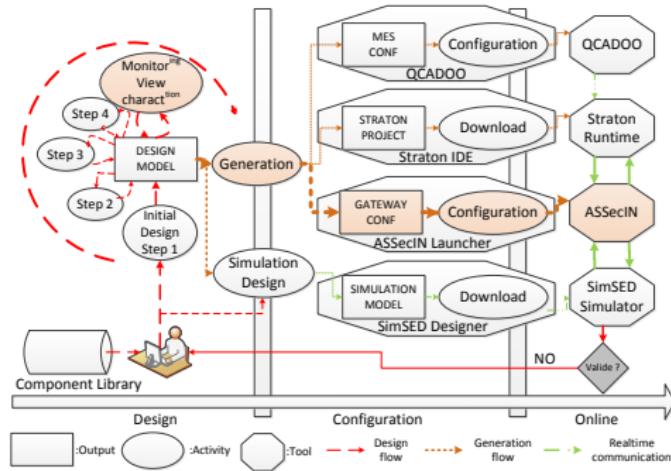


FIGURE – Flot global du projet

- Génération d'un fichier de configuration pour la passerelle
- Le concepteur instancie les contraintes de sécurité dans les composants
- (EN COUR) auto-génération de contrainte par transformation
- Le concepteur active les règles et valide les contraintes dont il a besoin

Auto-génération

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

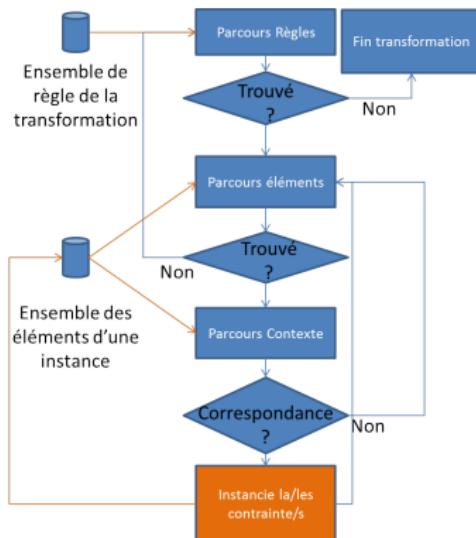


FIGURE – Description d'une transformation

- Lecture des règles de la transformation
- Lecture des éléments :
 - composant
 - opération
- Exploration du contexte de l'élément :
 - composant → opération
 - opération → composant(s) & paramètre
- Instantiation d'arbre binaire

Utilisation des vues :

- Topologique
- Matériel

Vues restantes :

- Contrainte

Règle de génération :

- Un composant ne peut voir que ses fils
- Les contraintes sont décomposées en 3 types :
 - ordres
 - environnement
 - mixte

Contexte

Recherche
Physique
Menace
Objectif &
problématique

Contribution

Description
de la
solution
Flot de
conception
Démonstrateur

Conclusion

Bilan
Perspective

Démonstrateur

Présentation du démonstrateur

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

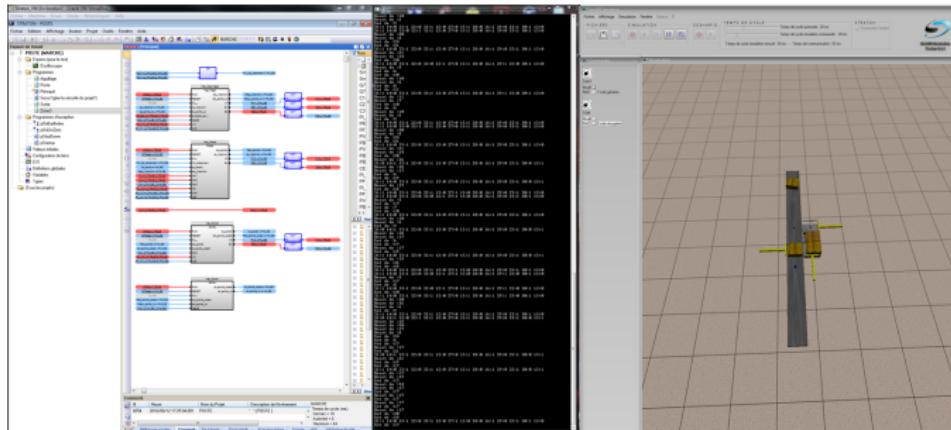


FIGURE – environnement du démonstrateur

Automate

- Emulé par runtime
- Code malicieux
- Scénario Rubber-ducky
- Attaque pilotée

Passerelle

- Log communication
- Log détection
- Sécurise process & alerte

Partie opérative

- Simulé par SimSED

Cas d'étude & résultat

ASSecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

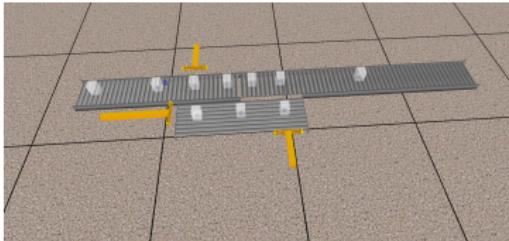


FIGURE – Cas d'étude

```

-----  

name : SSM_Systeme_secu_LV041  

ExType : safeTyr  

memoryAddress:0x392001  

=====LUZ : 0=====  

|order:Jack1_O_001  

|memoryAddress:0x392041  

|memorySize:4  

|segment AND  

| | AND | NOT | Jack1_O_00 | ONE | Stop_Ac_O_00  

| | false | false | false | false | false  

|order:Jack2_O_001  

|memoryAddress:0x392081  

|memorySize:4  

|segment OR  

| | OR | NOT | Jack2_O_00 | ONE | Stop_T_O_00  

| | false | false | false | false | false  

checking var: Jack1_O_00 with 5 Binary Tree  

the BT : 0 is validated  

the BT : 1 is validated  

the BT : 2 is validated  

the BT : 3 is validated  

the BT : 4 is validated  

exit from checking in 0s 29us  

checking var: Jack2_O_00 with 6 Binary Tree  

the BT : 0 is validated  

the BT : 1 is validated  

the BT : 2 is validated  

the BT : 3 is validated  

the BT : 4 is validated  

the BT : 5 is validated  

exit from checking in 0s 34us  

checking var: Jack1_O_00 with 5 Binary Tree  

the BT : 0 is validated  

the BT : 1 is not valid  

the BT : 2 is not valid  

the BT : 3 is not valid  

the BT : 4 is validated  

exit from checking in 0s 30us  

checking var: Jack2_O_00 with 6 Binary Tree  

the BT : 0 is validated  

the BT : 1 is validated  

the BT : 2 is not valid  

the BT : 3 is validated  

the BT : 4 is validated  

the BT : 5 is validated  

exit from checking in 0s 24us

```

FIGURE – Résultat

Cas d'étude

- 1 postes → 3ECC :
 - Intercepteur
 - Traitement
 - Ejecteur
- Utilisation de ComGEM & SecGEM
- Génération du code & de la configuration pour la passerelle

TABLE – Temporal analysis

essai	légère	lourde	moyenne
sans	32ms	42ms	37ms
avec	37ms	43ms	40ms
latence	5ms	1ms	3ms

Détection et latence

- La détection de l'attaque est effective
- La latence est minimale

Bilan fin de thèse

ASsecIN

Thomas
Toublanc

Contexte

Recherche

Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

TABLE – Bilan récapitulatif

axe	<i>partie</i>	<i>sous partie</i>	etat
Passerelle			88%
	mécanisme de détection	gardien safety	100% 100%
	mécanisme de réaction	log filtrage réécriture	75% 100% 50%
Flot			80%
	auto-génération détection		80%
		auto-génération BC auto-génération EBC auto-génération ECC auto-génération système	100% 100% 100% 20%
Démonstrateur	cas d'étude 1 poste	scénario bad automate	100% 100% 100%

Perspective

ASsecIN

Thomas
Toublanc

Contexte

Recherche
Physique

Menace

Objectif &
problématique

Contribution

Description
de la
solutionFlot de
conception

Démonstrateur

Conclusion

Bilan

Perspective

Passerelle

- Nx mécanismes détection-réaction
- Optimisation passerelle pour :
 - Multi-architecture
 - Multi-niveaux
 - Multi-protocole
 - L'hyper-com_{tion} & l'admin_{tion} I4.0

Flot

- Auto-génération → nx mécanismes
- Auto-génération → communication
- Auto-génération → haut niveau
- Adaptation à l'industrie du futur

Démonstrateur

- Nouveaux cas d'étude
- Test des nouveaux mécanismes
- Simulation d'usine réel en virtuel

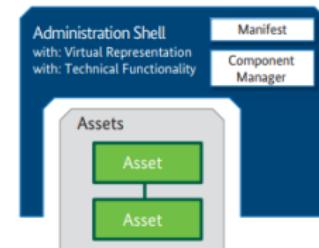


FIGURE – Shell d'administration [AIF (2018)]

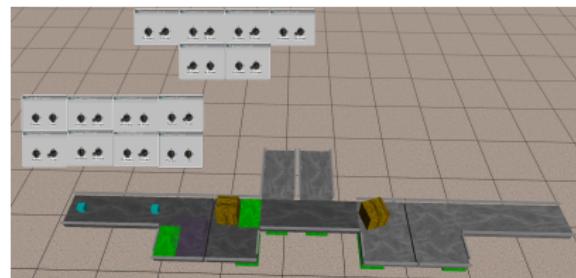


FIGURE – Nouvelle ligne SCAP

Conclusion

ASSecIN

Thomas
Toublanc

Contexte

Recherche
Physique
Menace
Objectif &
problématique

Contribution

Description
de la
solution
Flot de
conception
Démonstrateur

Conclusion

Bilan
Perspective

Merci de votre attention
Avez vous des questions ?