Détection dans les systèmes industriels: Suricata et le cas Modbus

Conférence C&ESAR

David DIALLO et Mathieu FEUILLET

{mathieu.feuillet,david.diallo}@ssi.gouv.fr

25 novembre 2014

ANSSI

ANSSI : Agence nationale de la sécurité des systèmes d'information
Autorité nationale de cyberdéfense, services du premier ministre

Trois missions principales :

- **Défendre**
- **Prévenir**
- **Informer**

`http://www.ssi.gouv.fr/`

Systèmes industriels

Définition : système d'information ayant des actions physiques.

Constat : mêmes vulnérabilités et de plus en plus visés.

Spécificités des systèmes industriels

Besoins de sécurité :

1. Intégrité
2. Disponibilité
3. Confidentialité (optionnel)

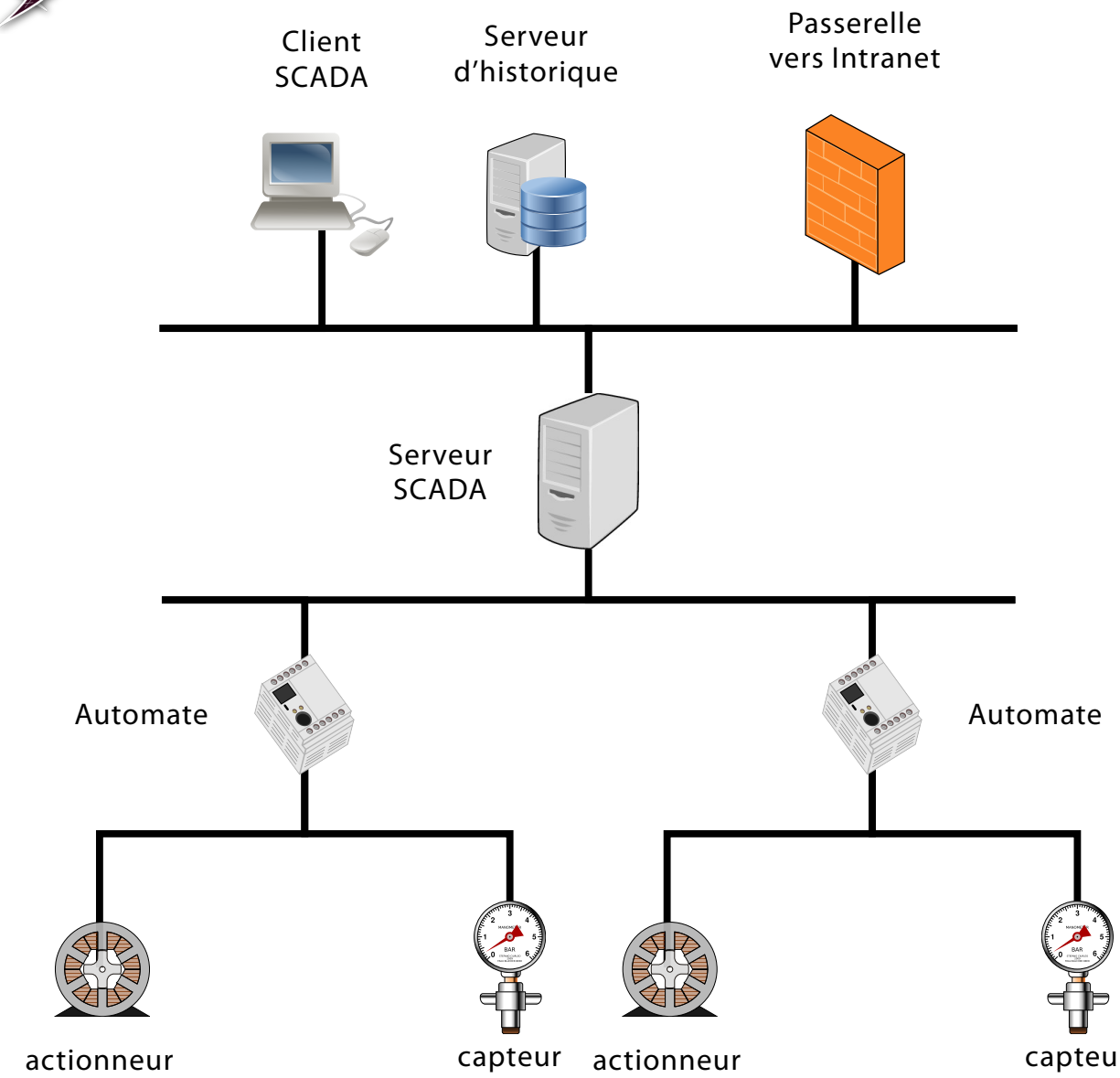
Contraintes :

- Durée de vie élevée
- Fonctionnement en continu avec arrêts planifiés
- Pour certains, contraintes de temps de réponse

Atouts :

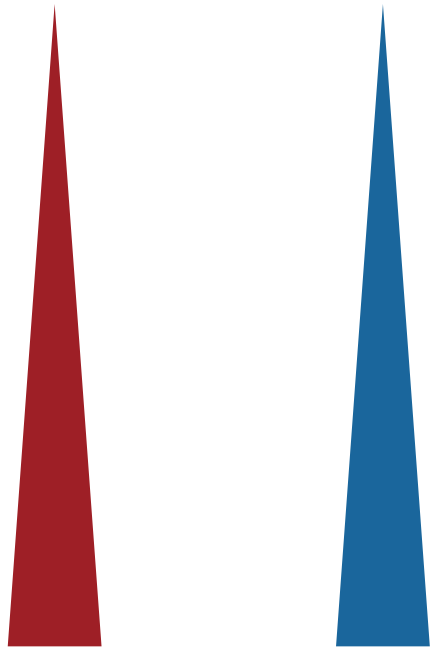
- Architecture (souvent) bien définie
- Comportement cadré et limité
- Evolution lente (peu de modifications)

Architecture typique



Disponibilité Technologie
Intégrité

Critique Standard



Très critique Spécifique

Systèmes de détection

Système de détection d'intrusion **IDS**

- dispositif de sécurité issu des systèmes d'information de gestion
- analyse le trafic réseau

SCADA sécurité

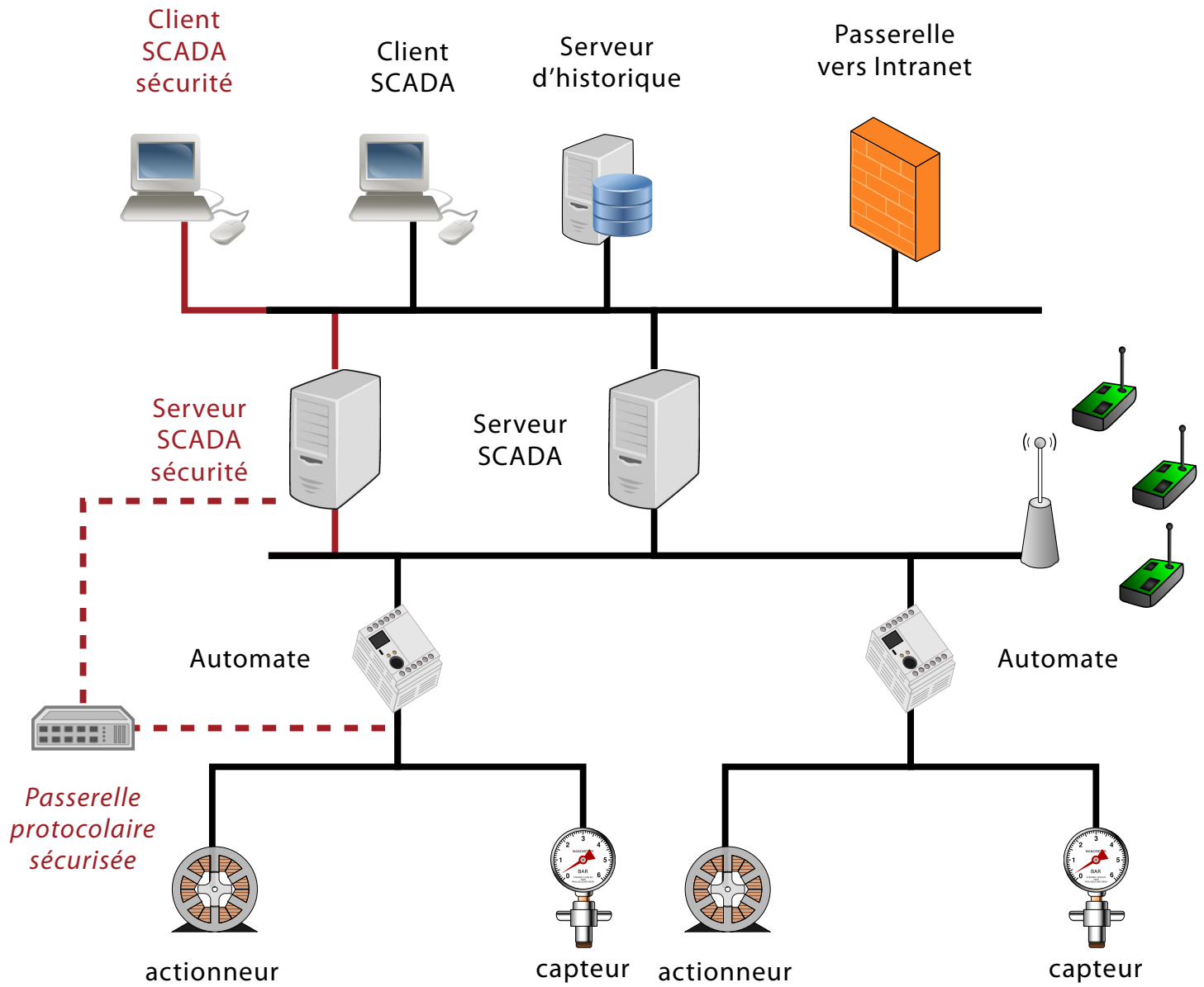
- issu des systèmes industriels
- collecte active de l'information (monitoring)
- complément à la supervision du procédé industriel

SCADA sécurité : Que détecter ?

Détection par ordre d'importance

1. Sortie de bornes du procédé industriel
2. Suivi et collecte des informations système
   - Connexion et déconnexion d'utilisateur
   - Charges CPU
   - Compteurs (de trames…)
3. Incohérence des informations
   - Corrélation entre sources

SCADA sécurité : Où détecter ?

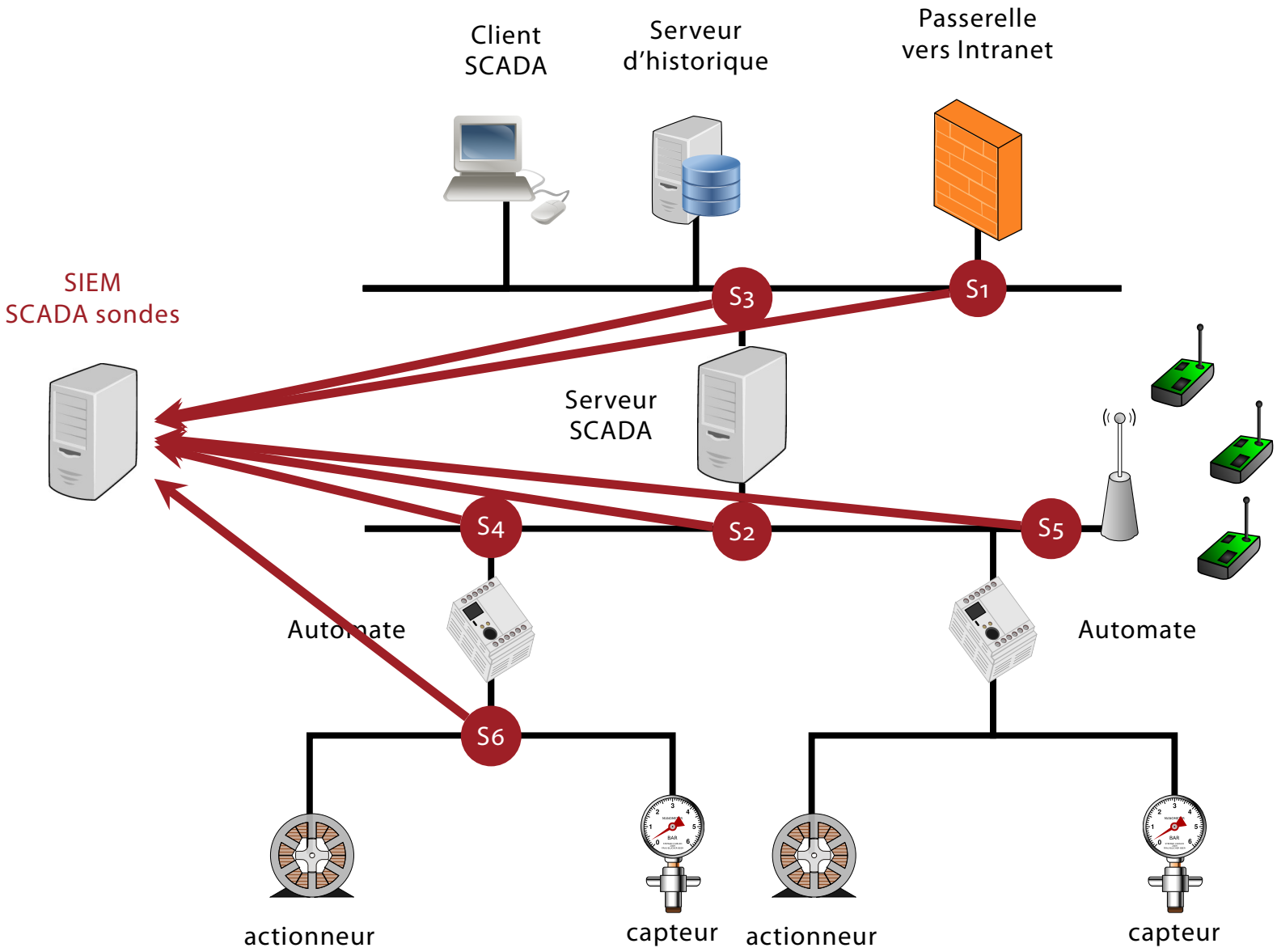


IDS : Que détecter ?

Détection en fonction de la maturité

1. Détection d'évènements simples redoutés
   - Reprogrammation d'automate (StuXnet)
   - Ordre d'arrêt
   - Vulnérabilités connues (CVE)
   - Conformité protocolaire
2. Violation de la matrice de flux
3. Violation de la politique de sécurité
   - Utilisation de fonctions illicites
   - Dépassement de seuils
   - Écriture hors des zones autorisées
4. Détection en liste blanche

IDS : Où détecter ?



SCADA sécurité vs IDS

SCADA sécurité

Atouts

- Collecte d'alarme, de valeurs et d'évènements systèmes
- Analyse des évènements dans le temps
- Corrélation entre sources
- Formation et appropriation accélérées (mêmes outils…)

Défauts

- Intrusif
- Mise à jour délicate

IDS

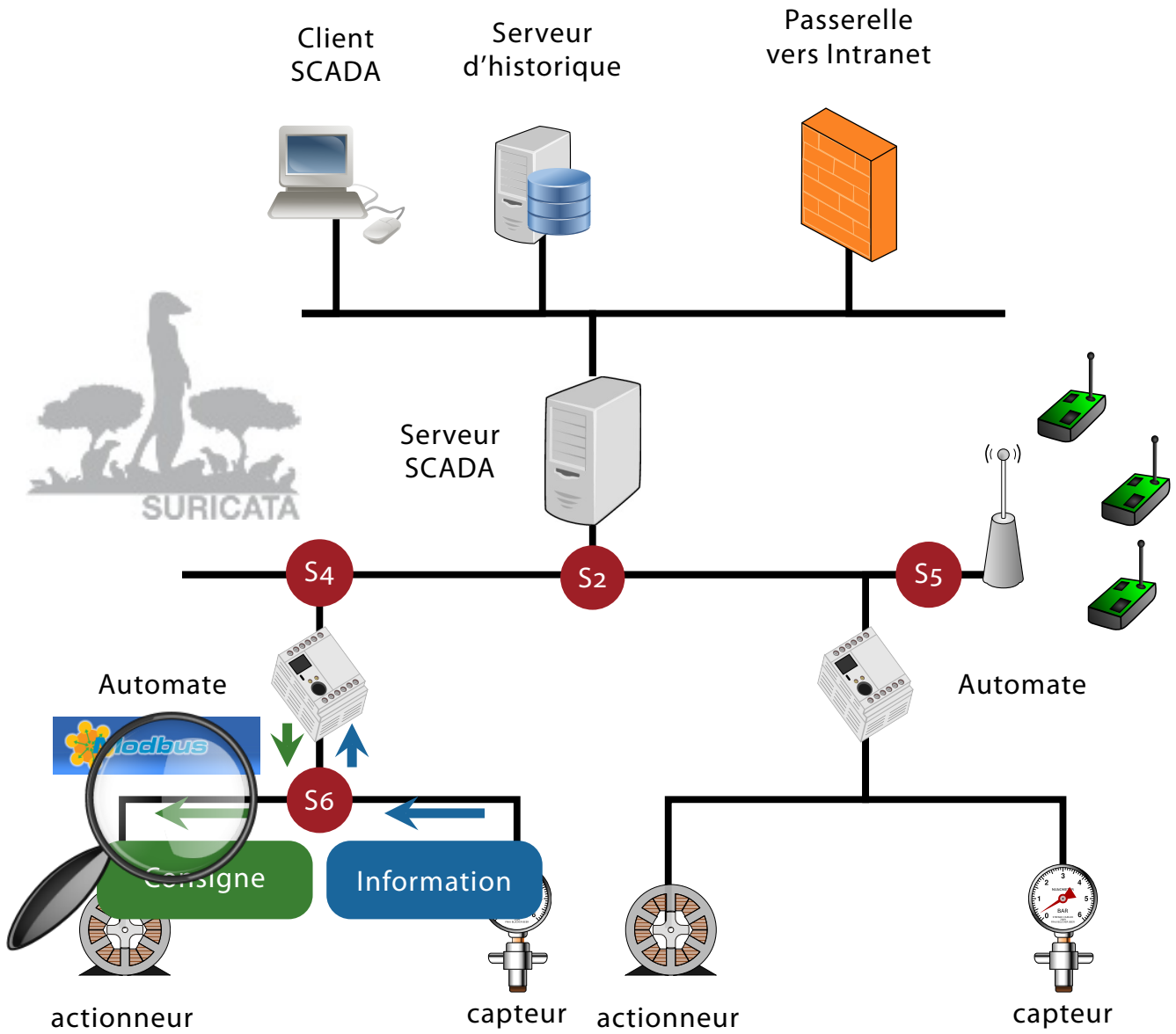
Atouts

- Système non intrusif
- Préexistence d'une surveillance par des opérateurs
- Trafic réseau exhaustif au point de collecte
- Mise à jour plus aisée et moins risquée

Défauts

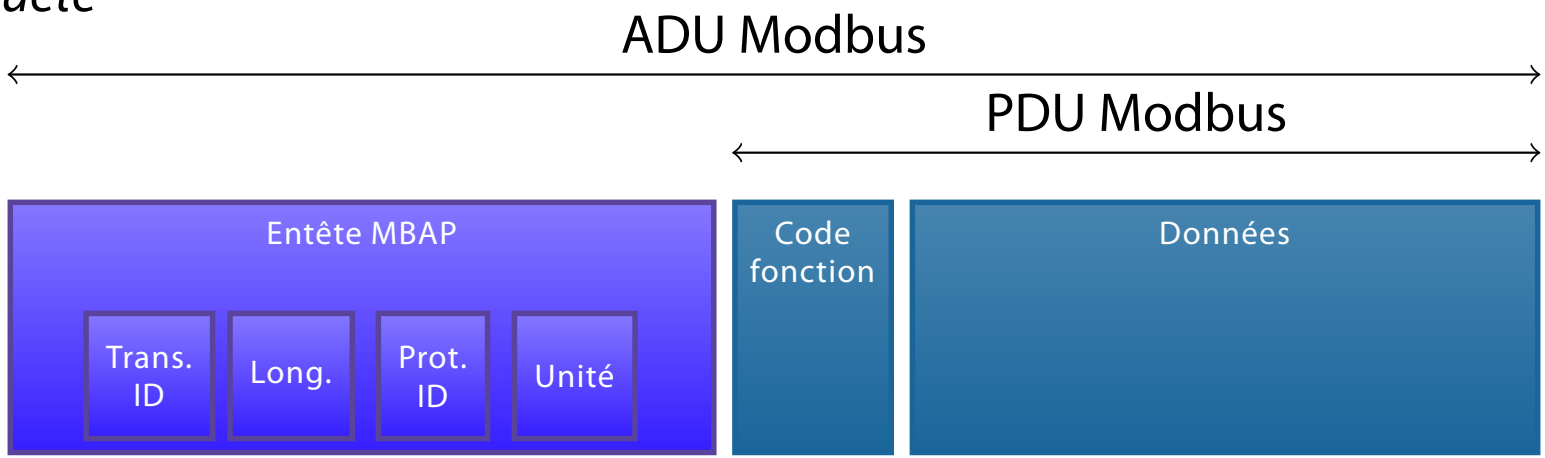
- Maintien à jour nécessaire

Cas pratique

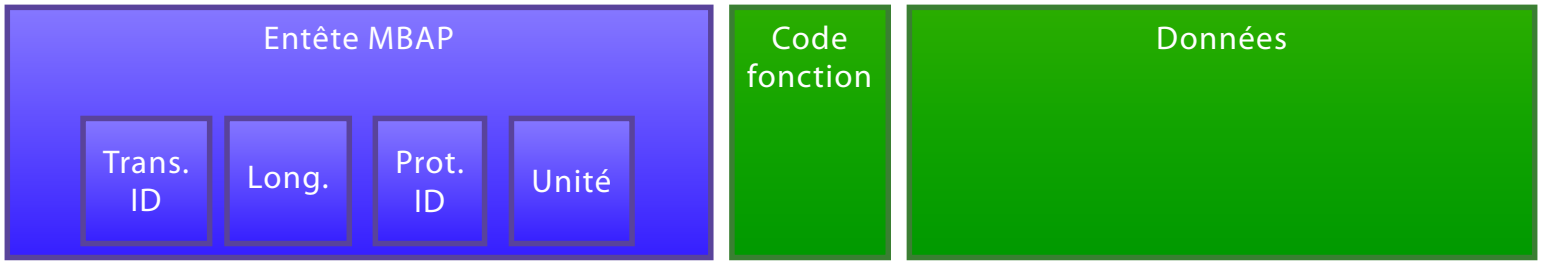


Protocole Modbus TCP/IP

Requête



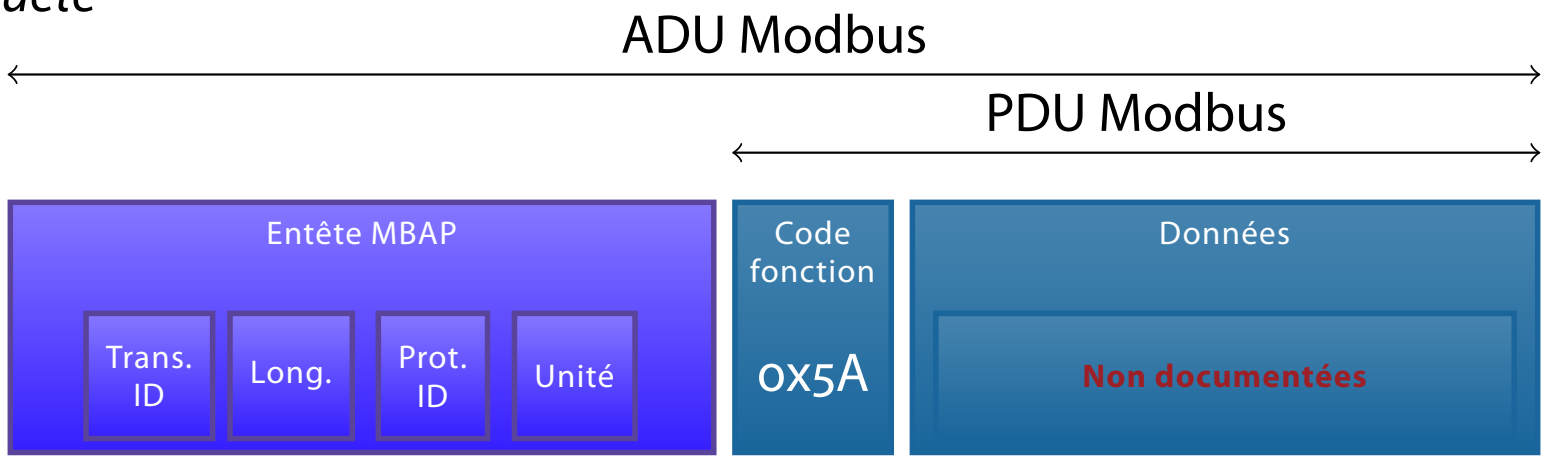
Réponse



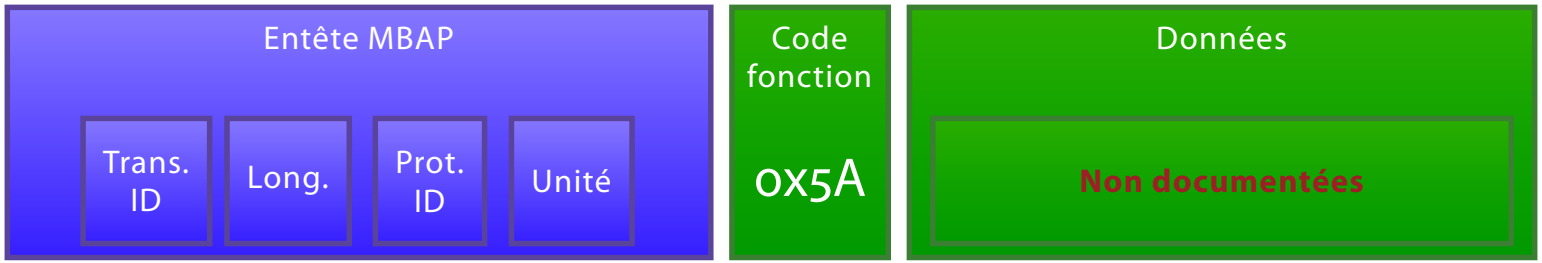
Exemple 1 : Extension Modbus UMAS

Extension Modbus UMAS : Fonction réservée Schneider Electric

Requête



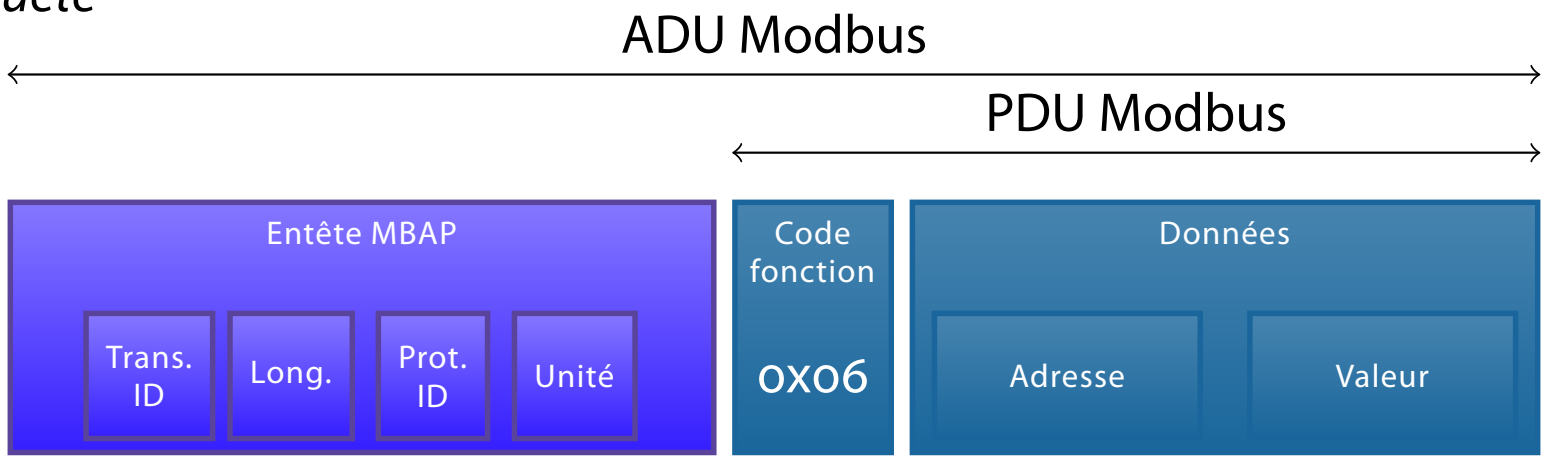
Réponse



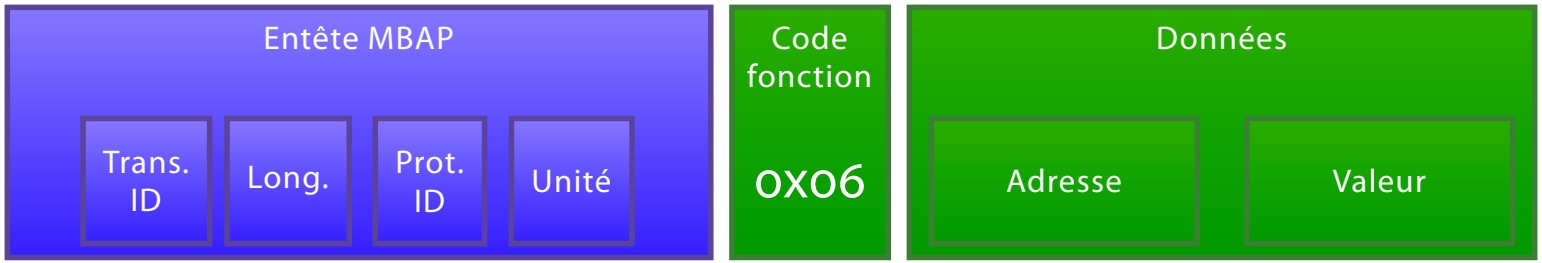
Exemple 2 : Écriture dans un registre

Fonction Write Single Register : Écriture dans un registre

Requête



Réponse



Suricata : Détection de motif

Exemple 1 : Protocole Modbus UMAS

```
alert tcp $MODBUS_CLIENT any -> $MODBUS_SERVER 502
        (content:"|5A|"; offset:7; depth:1;
    msg:"Modbus TCP - Modbus UMAS Protocol"; [...])
```

Limitations :

- Possibilité de contourner l'IDS
- Pas de vérification de la conformité
- Complexité d'implémentation des règles plus précises

Contribution Suricata : Préprocesseur Modbus

Exemple 1 : Protocole Modbus UMAS

```
alert modbus $MODBUS_CLIENT any -> $MODBUS_SERVER any

        (modbus.function: 0x5A;
    msg:"Modbus TCP - Modbus UMAS Protocol"; [...])
```

Avantages :

- Définition moins complexe et plus performante des règles
- Vérification de la conformité du protocole

Contribution Suricata : Préprocesseur Modbus

Exemple 1 : Protocole Modbus UMAS

```
alert modbus $MODBUS_CLIENT any -> $MODBUS_SERVER any

(modbus.function: reserved;
msg:"Modbus TCP - Reserved function"; [...])
```

Avantages :

- Définition moins complexe et plus performante des règles
- Vérification de la conformité du protocole
- Définition étendue

Contribution Suricata : Préprocesseur Modbus

Exemple 2 : Écriture dans un registre

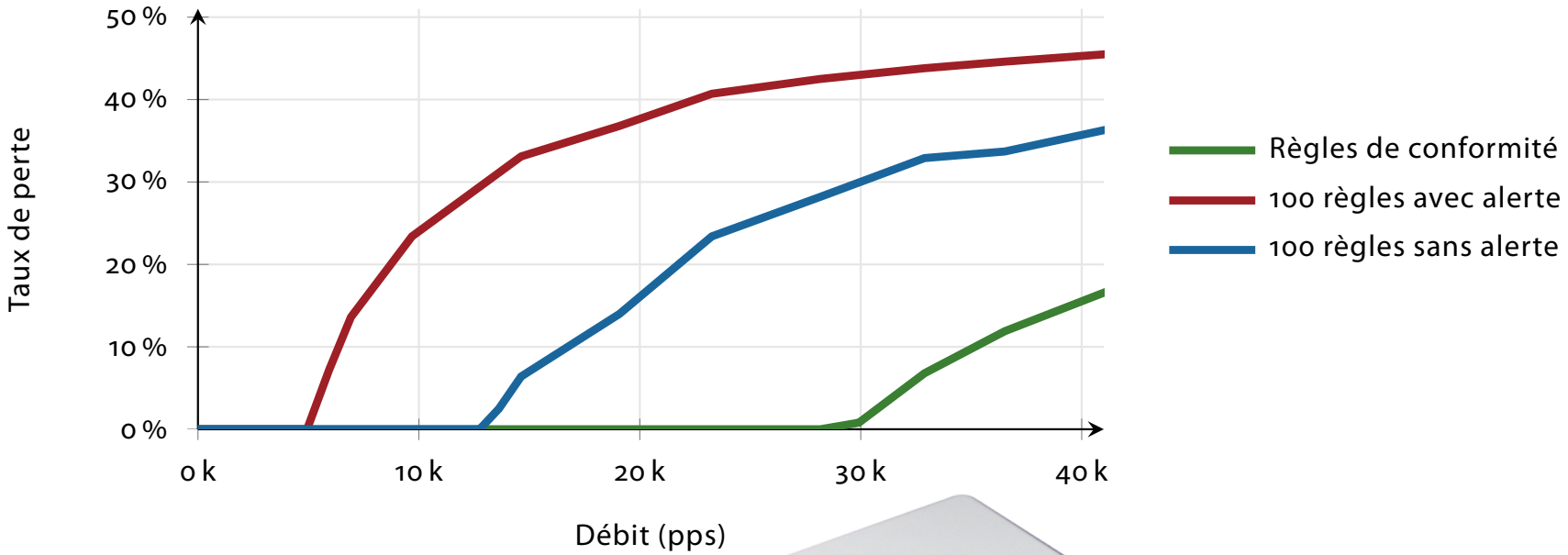
```
alert modbus $MODBUS_CLIENT any -> $MODBUS_SERVER any
        (modbus.access: write holding,
          address 100, value >2000;
      msg:"Vitesse moteur trop élevée"; [...])
```

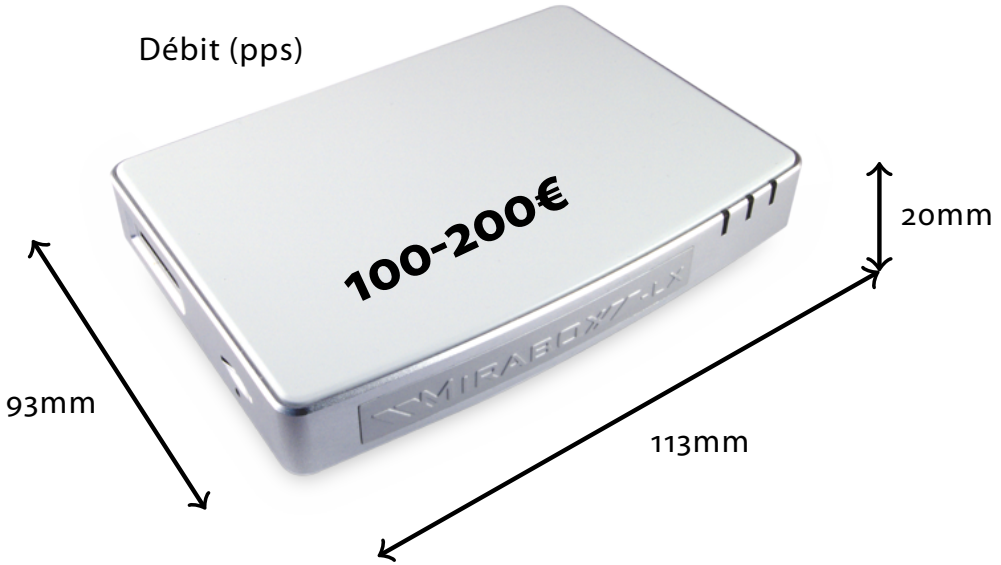
Avantages :

- Définition moins complexe et plus performante des règles
- Vérification de la conformité du protocole
- Définition étendue
- Vérification du contenu

Performance

Métrique de performance d'un IDS : taux de perte.





Conclusion

1. Deux méthodes de détection complémentaires :
   - SCADA sécurité
   - IDS
2. Passivité de l'IDS adaptée aux anciens systèmes
3. Code disponible Suricata V2.1 beta3
   `https://github.com/inliniac/suricata/`

Perspectives :

- D'autres protocoles industriels (S7, EtherNet/IP…)
- Quid de la sécurité des sondes IDS ?