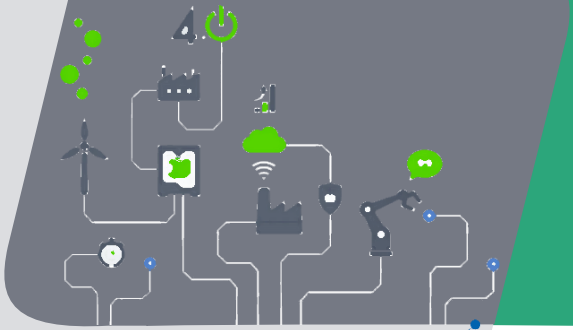
PROFIBUS • PROFINET



Fonctions de sécurité et Serveur de Sécurité pour ICS

PROFINET PROFIBUS PROFIsafe PROFIenergy PROFIdrive IO-Link FDI

Cas d'usage considéré

- ICS hétérogène
  - Authentification propre à chaque application
  - Fonctions de sécurité partielles (journaux d'évènements, analyse des flux….)
  - Segmentation insuffisante et non contrôlée
- Maintien en Conditions de Sécurité difficile à mettre en œuvre
  - Cartographie et nomenclature insuffisante ou non à jour
  - Alertes de sécurité versus vulnérabilités réelles : comment ?
  - Journalisation, back-up et restauration faiblement utilisables dans un contexte de malveillance
- Interfaces IT – OT
  - Accès distant … plus ou moins sécurisé
  - Administration de l'ICS
  - Besoin d'échanges opérationnels et de mise à jour

Problématique à réponse multiple

- Sécurité intrinsèque des composants (équipements ou logiciels) versus équipements de sécurité système indépendants
- Importance des architectures physiques, logiques et fonctionnelles
- Fonctions de sécurité essentielles ou accessoires ?
- Priorités ?
- Interdépendance avec les mesures organisationnelles
- Qui sont les acteurs de la cybersécurité industrielle ?
- Comment faire évoluer la sécurité tout au long de l'utilisation de l'ICS ?
- Qu'est-ce qui est couvert par la sûreté de fonctionnement ?

Intérêts d’un serveur de sécurité

- Un élément exogène, système
- Propose des services de sécurité adaptés aux différents composants de l’ICS
- Permet de rendre beaucoup plus difficile l’intrusion dans un ICS ou l’exploitation de ses vulnérabilités
- Concentre des technologies classiques du monde de l’IT

Exemple de fonctions d’un serveur de sécurité


Firewalls


Segmentation
des sous-réseaux


Serveur d’authentification


Serveur anti-virus


Back-up & Disaster recovery


Enregistrement et restitution des
évènements de sécurité


Virtualisation d’applications


Sonde de détection d’intrusion


Diode réseau

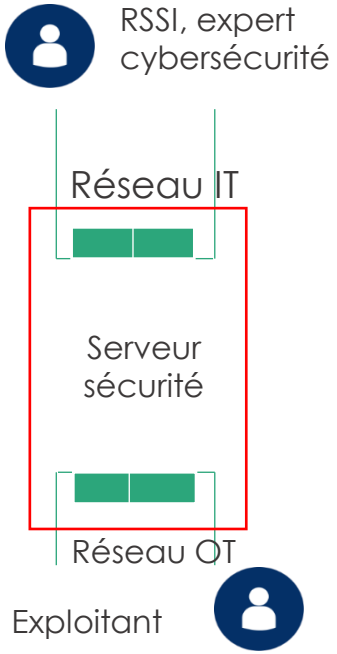

Administration des redondances

Considérations pratiques… et gênantes

- Fourni par le constructeur ICS ou indépendant ?
- Administré comment ? Et par qui ?
- Lien avec les fonctions de sécurité IT ? (annuaire pour l'authentification, serveur d'anti-virus, récupération des logs…)
- Robustesse et confiance de ce serveur ?
- Adaptation des composants de l'ICS ?

Exemple de serveur intégré dans une DMZ

- Assure une communication sécurisée entre le réseau à protéger OT et l'IT
- Défense en profondeur : plusieurs firewall à traverser
- Ne laisse rien passer, sauf ce qui est légitime: principe de white list
- Chacun gère son interface IT et OT et les services dont il a la charge
- Mise en place de services partagés par l'IT et l'OT
- Modèle de firewall au choix du client
- Cloisonnement horizontal



Couverture des exigences de sécurité (1/2)

IEC 62443 3-3 Exigences fondamentales	Loi de Programmation Militaire	ANSSI – Mesures détaillées de sécurité	Apports serveur de sécurité
FR1 – Contrôle de l'identification et de l'authentification	11 – Identification 12 – Authentification 13 – Droits d'accès 14- Comptes d'administration	4-1 Authentification des intervenants	Mise à disposition d'un système d'identification et d'authentification pour toutes les applications OT Synchronisation avec l'annuaire IT Administrable par un RSSI
FR-2 –Contrôle de l'utilisation	5 – Journalisation des évènements 7- Détection par sonde d'analyse de fichiers et de protocoles	4-2 Sécurisation de l'architecture du système industriel	Enregistrement de tous les évènements d'exploitation et de sécurité liés aux services administrés Gestion de sessions Intégration de la sonde détection d'intrusion Services locaux (ingénierie, maintenance) disponibles à distance via proxy
FR3 – Intégrité du sytème	4 – Maintien en conditions de sécurité 19 – Installation de services et d'équipements	4-3 Sécurisation des équipements	Anti-virus Whitelisting Récupération des évènements et indicateurs (SNMP, syslog…) des équipements OT et analyse locale
FR4 – Confidentialité des données			Enregistrements chiffrés et protocoles d'échanges sécurisés vers le monde IT

Couverture des exigences de sécurité (2/2)

IEC 62443 3-3 Exigences fondamentales	Loi de Programmation Militaire	ANSSI Mesures détaillées de sécurité	Apports serveur de sécurité
FR5 – Restriction concernant les échanges	16 –Cloisonnement 17- Filtrage	4-2 Sécurisation de l'architecture du système industriel	Cloisonnement Protection de l'interconnexion IT et des accès distants
FR6 – Réponse aux évènements dans les temps	4 – Maintien en conditions de sécurité 5- Détection par sonde d'analyse de fichiers et de protocoles 6 – Corrélation et analyse des journaux	4-3 Sécurisation des équipements 4-4 Surveillance du système industriel	Analyse des échanges sur le réseau par la sonde de détection d'intrusion Coordination entre la sonde de détection et un SIEM Enregistrements de sécurité disponible pour une analyse post-incident Interface spécifique RRSI avec administration à distance
FR7 – Disponibilité des ressources	19 – Installation de services et d'équipements 4 – Maintien en conditions de sécurité	A - Cartographie	Back-up des programmes et des configurations Détection de modification des programmes automates Capacité à monter les applications niveau 2 (supervision- ingénierie - ordonnancement – archivage) en machines virtuelles, avec redondance et restauration en temps réel

Conclusion

- Un serveur de sécurité permet d'apporter rapidement des mesures efficaces
- Minimise les impacts sur l'ICS lui-même
- Ne nécessite pas d'analyse de risque poussée
- Permet un dialogue constructif entre le monde IT et OT au sujet de la sécurité informatique.