Cybersécurité des systèmes industriels : des solutions

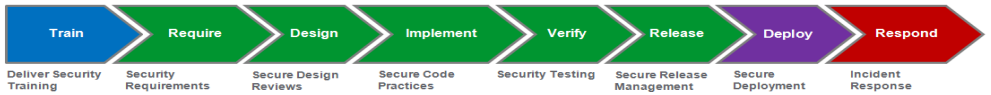
Schneider Electric – Novembre 2020

Yann Bourjault, Directeur Transformation Digitale & Cybersécurité France

Le programme Cybersécurité de Schneider Electric

Les 4 piliers du programme

Spécifications basées sur des standards



Développés suivant un process Secure Development Lifecycle (SDL)

Produits cœurs

Produits de sécurité

Ecosystème de partenaires pour proposer les meilleures solutions adaptées au monde industriel

HIRSCHMANN A BELDEN BRAND

STORMSHIELD

THALES

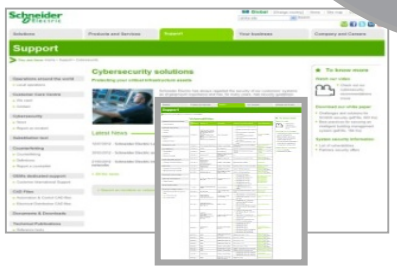
KUB

WALLIX TRACE,AUDIT&TRUST

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

Recommandations de mise en œuvre

Informations sur les vulnérabilités



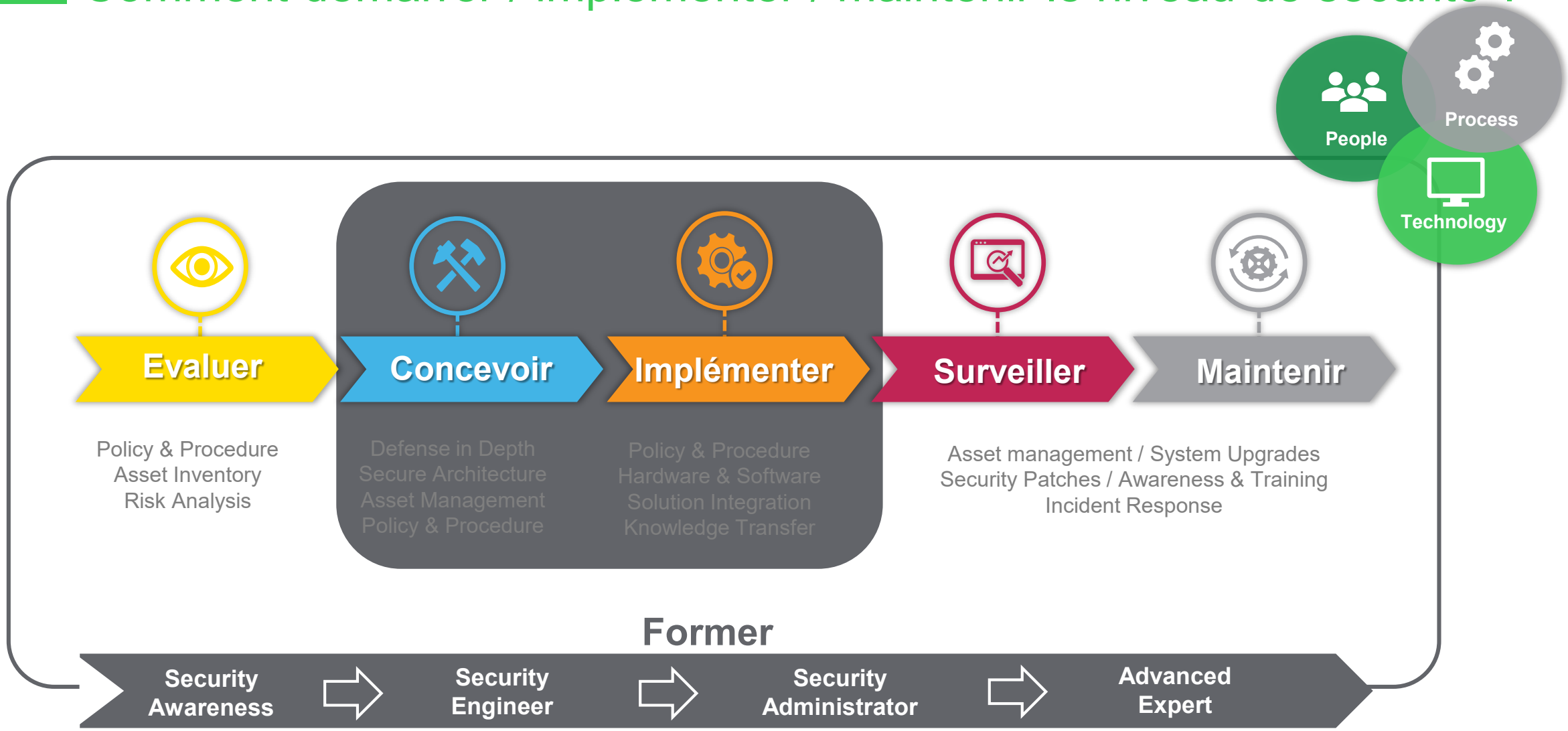
Centre de compétences

Services Cyber sécurité

Menés par des experts en cyber sécurité connaissant votre environnement industriel

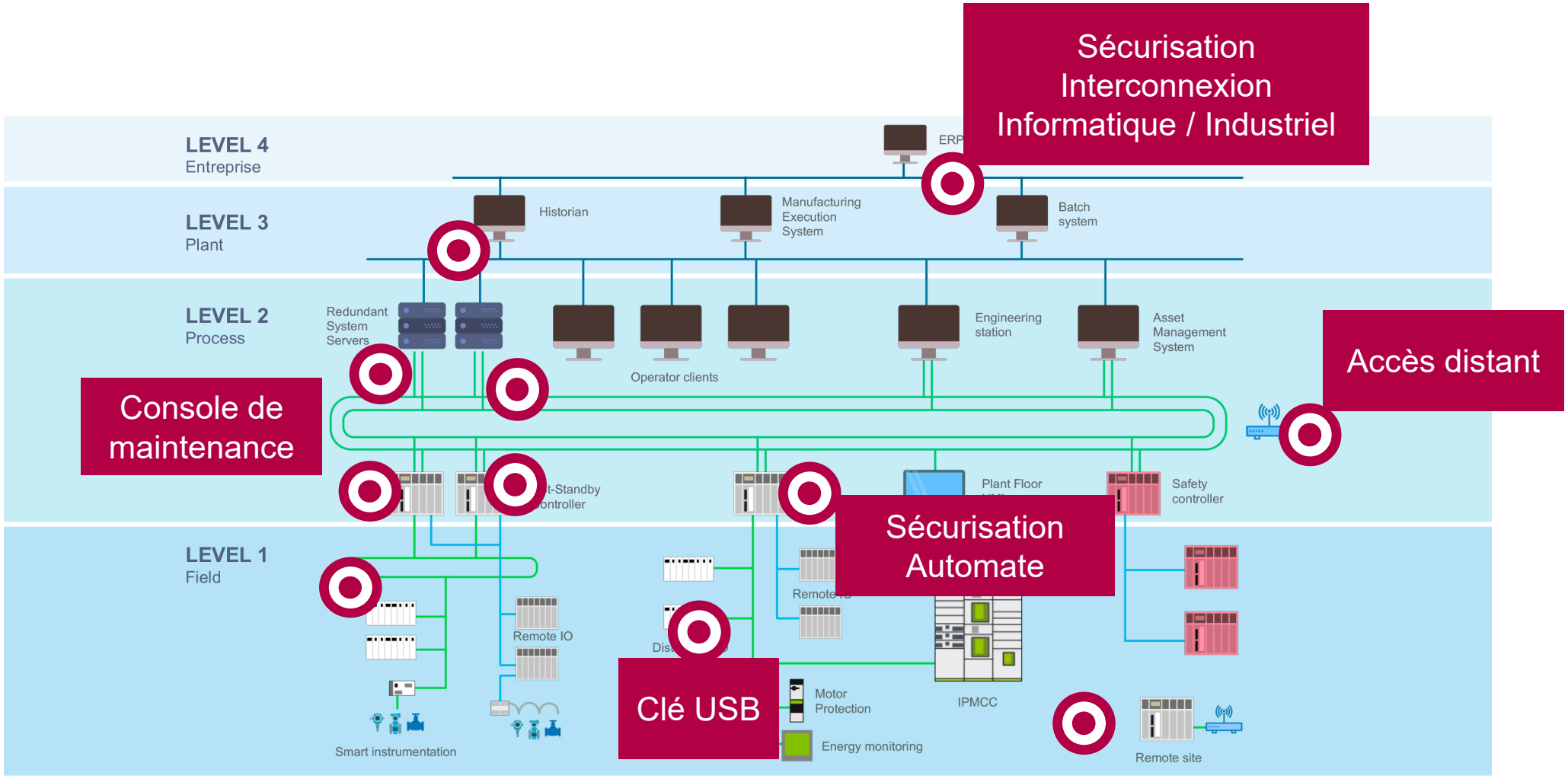
Life Is On Schneider Electric

Comment démarrer / implémenter / maintenir le niveau de sécurité ?



Life Is On Schneider Electric

Principaux vecteurs d’intrusion



niveaux selon le modèle ISA95

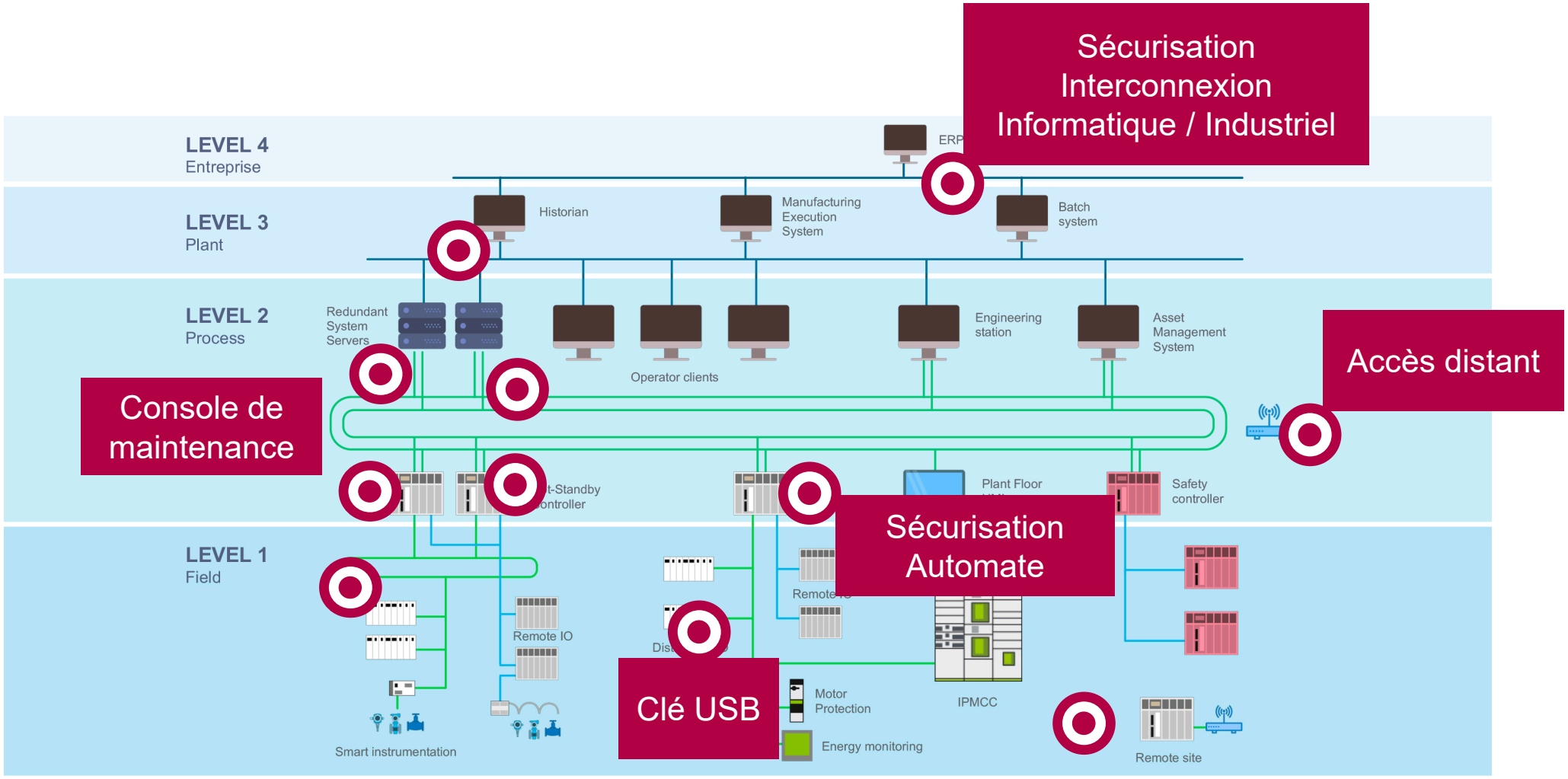
Automate M580 : L'automate Schneider Electric certifié ANSSI

Certification Achilles L2 et ANSSI CSPN

Robustesse
de la communication

- **Intégrité Système, Firmware, et Software**
  - Vérifications système temps réel :
    processeur, mémoire, tâches système
  - Firmware M580 signé et crypté :
    algorithmes SHA256 – RSA4096 – AES256
  - Logiciel signé, vérifiable à tout moment
- **Contrôles d'accès renforcés**
  - Désactivation des services inutilisés:
    HTTP, FTP, EIP, DHCP, BOOTP, SNMP, etc.
- **Communication sécurisée**
  - Le protocole IPSEC pour sécuriser
    la communication entre un PC et l'automate

Principaux vecteurs d’intrusion



niveaux selon le modèle ISA95

Console de maintenance sécurisée Cybertec

La Cybertec répond au guide des mesures détaillées de l'ANSSI :

Directive 258 : Les consoles de programmation devraient :

- **Ne pas être connectées à Internet**
- **Etre en mesure de procéder à la désactivation des composants inutiles**

Directive 217 : Des outils de défense en profondeur du poste de travail devraient être mis en place. En particulier, **une liste blanche des applications ayant le droit de s'exécuter** devrait être mise en place sur les équipements.

Directive 236 : **Des médias amovibles dédiés** aux systèmes industriels devraient être mis à disposition des intervenants.

Directive 251 : Lorsque l'équipement contient des données sensibles, **sa mémoire de stockage devrait être chiffrée.**

Détail des mesures de protection

Le système d'exploitation, les applications et les données sont protégées par 6 outils

1. Contrôle des utilisateurs
2. Contrôle des exécutables
3. Contrôle des périphériques
4. Chiffrement
5. HIPS
6. Firewall

Les politiques d'accès aux périphériques, d'exécution d'applications, de mise à jour, etc… sont dynamiques en fonction de l'utilisateur authentifié.

L'utilisateur « Operateur » est un utilisateur standard alors que l'utilisateur « Administrateur » a des droits complets d'administration.

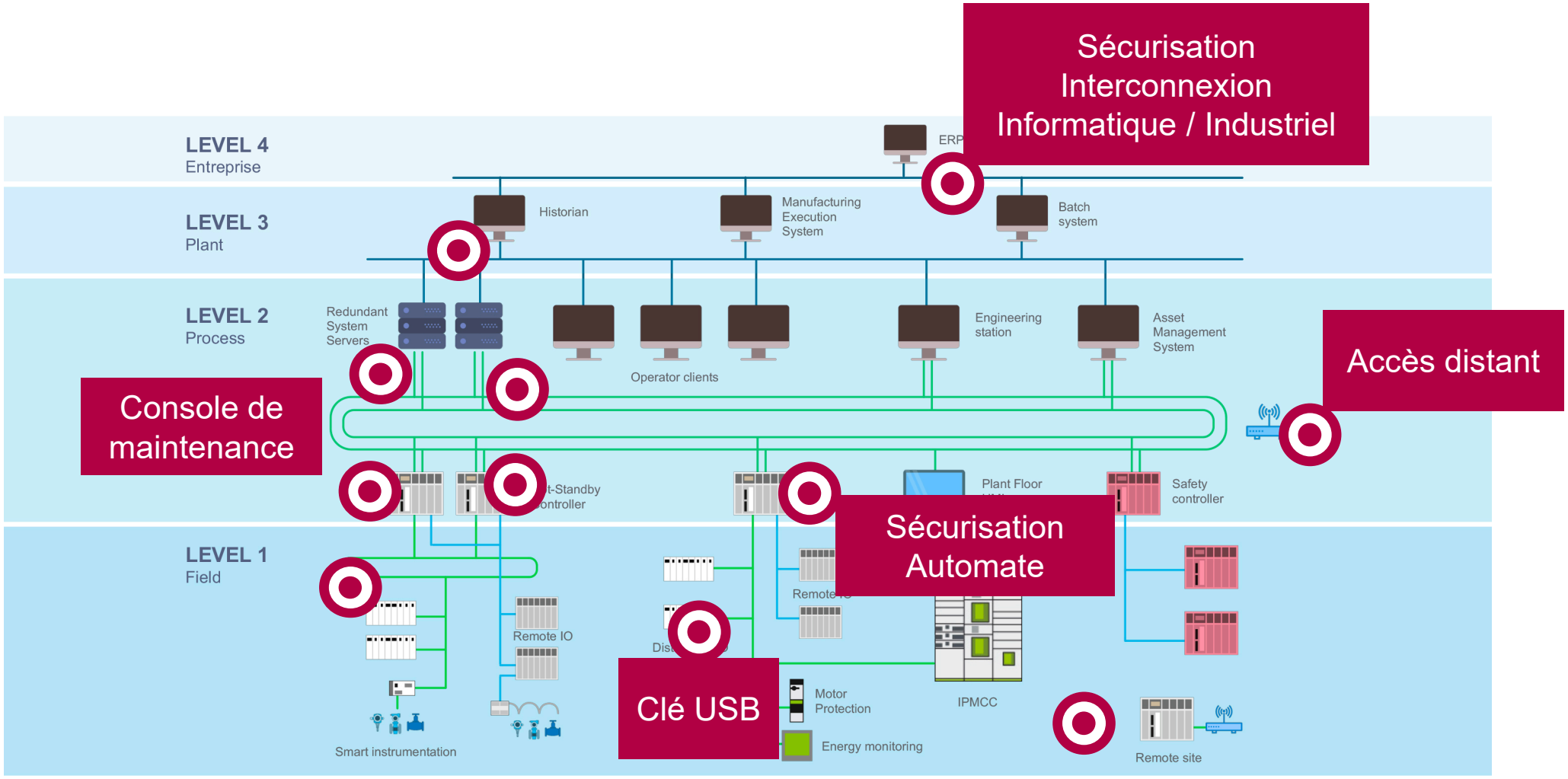
Détail des mesures de protection

Le système d'exploitation, les applications et les données sont protégées par 6 outils

1. Contrôle des utilisateurs
2. Contrôle des exécutables
3. Contrôle des périphériques
4. Chiffrement
5. HIPS
6. Firewall

Afin de garantir la confidentialité des données contenues sur le disque dur, celui-ci est chiffré en AES 256 avec la solution Cryhod qualifiée ANSSI. La clé de chiffrement est stockée dans la puce TPM (Trusted Platefom Module) de la carte mère.

Principaux vecteurs d’intrusion



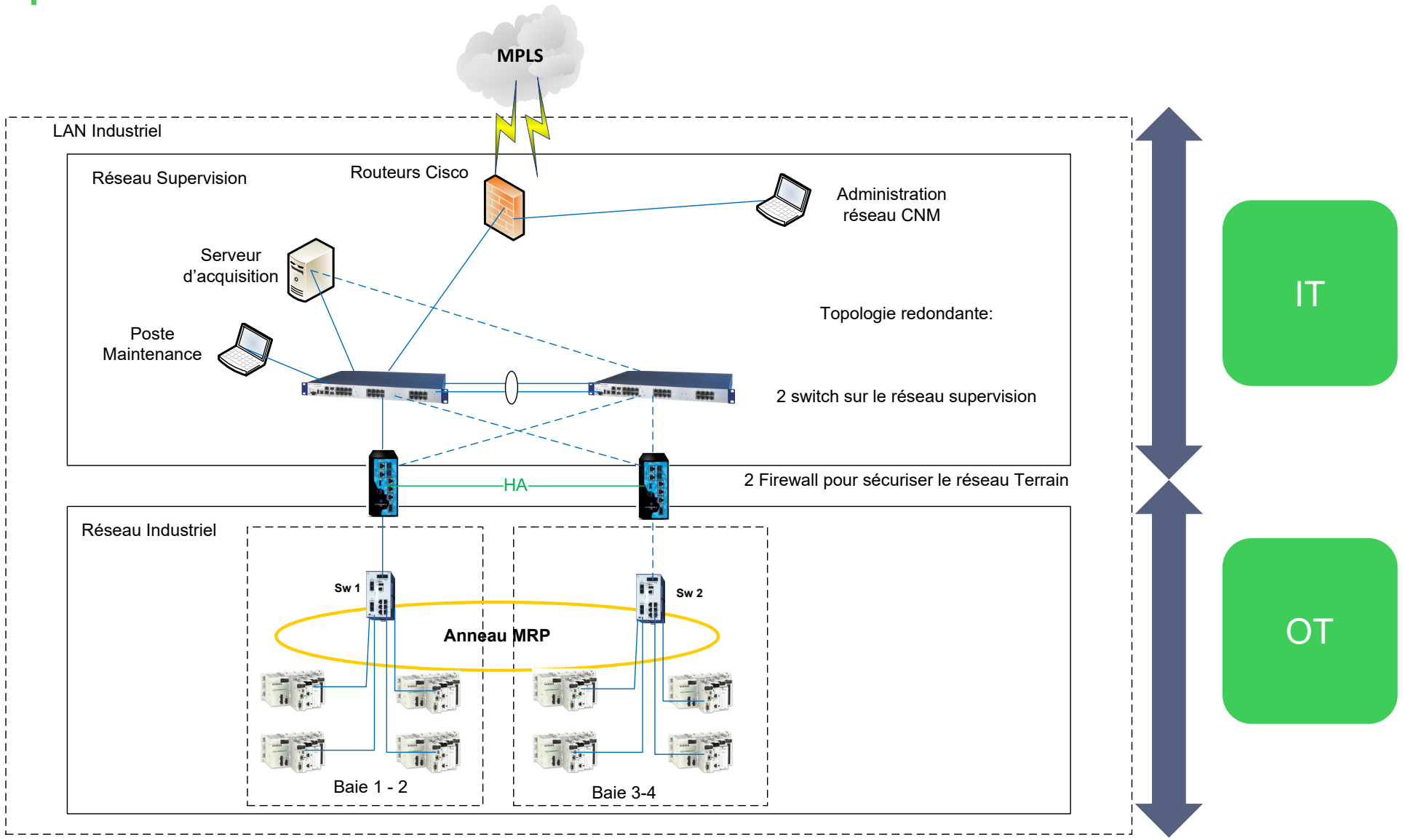
niveaux selon le modèle ISA95

Pare-feu SNi40 : adapté aux contraintes industrielles

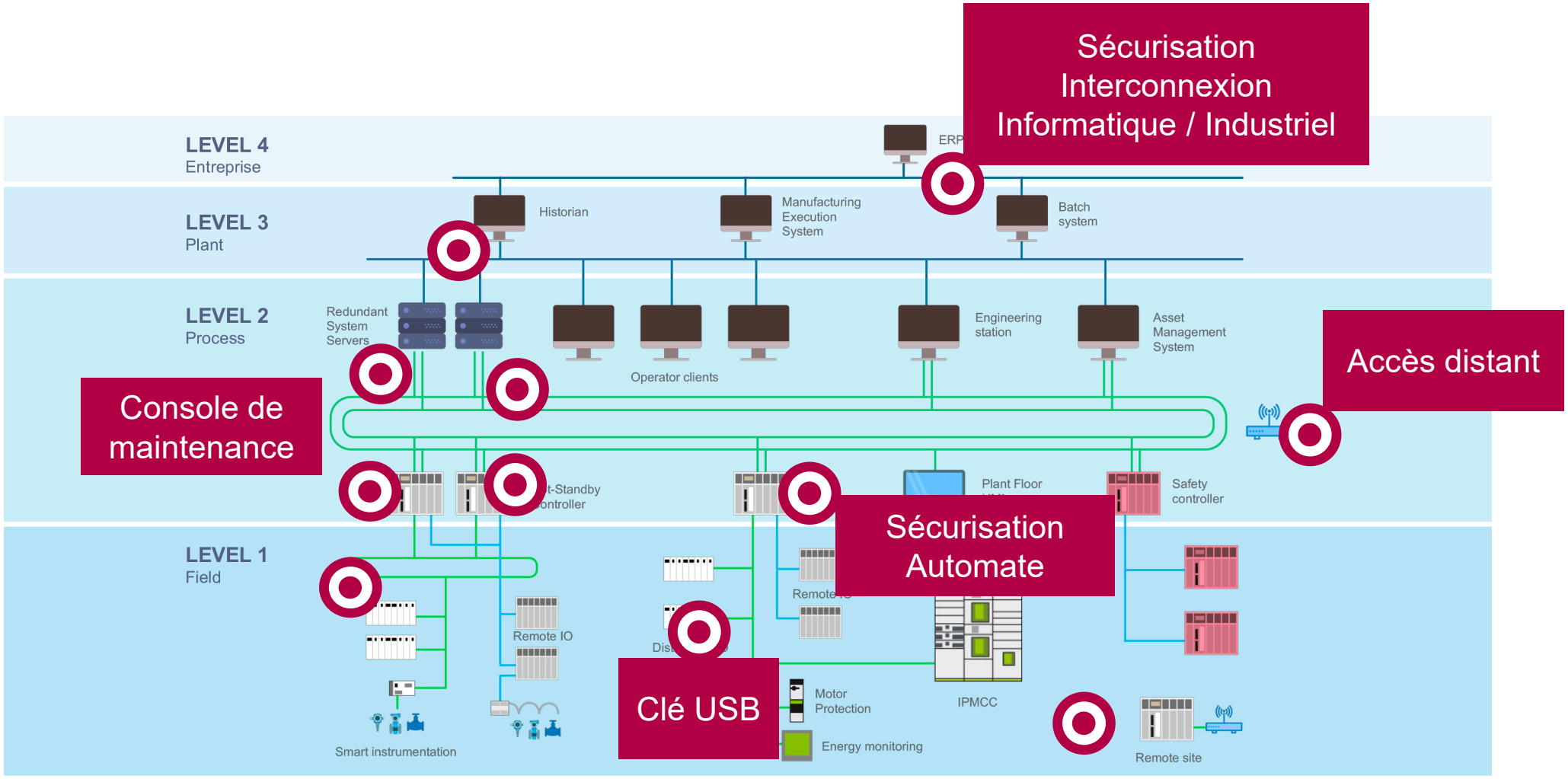
- STORMSHIELD : **Une expérience de 15 ans dans la cyber sécurité réseau**
- Développé dans le cadre du projet NG-IUTM, partenariat **Stormshield/Schneider Electric** commandité par l'ANSSI
- **Certifié et Qualifié CSPN**
- **Une formation et certification** unique IT/OT
- **Solution de détections** des vulnérabilités réseaux
- **DPI des Protocoles Industriels** :
  Modbus, S7, OPC UA, IEC104, OPC DA, Ethernet/IP

Depuis mai 2016 : **+ de 50 industriels d'infrastructures sensibles** équipés et formés

Exemple d'architecture : Sécurisation Interconnexion IT/OT



Principaux vecteurs d’intrusion



niveaux selon le modèle ISA95

Station de décontamination USB multi-antivirus

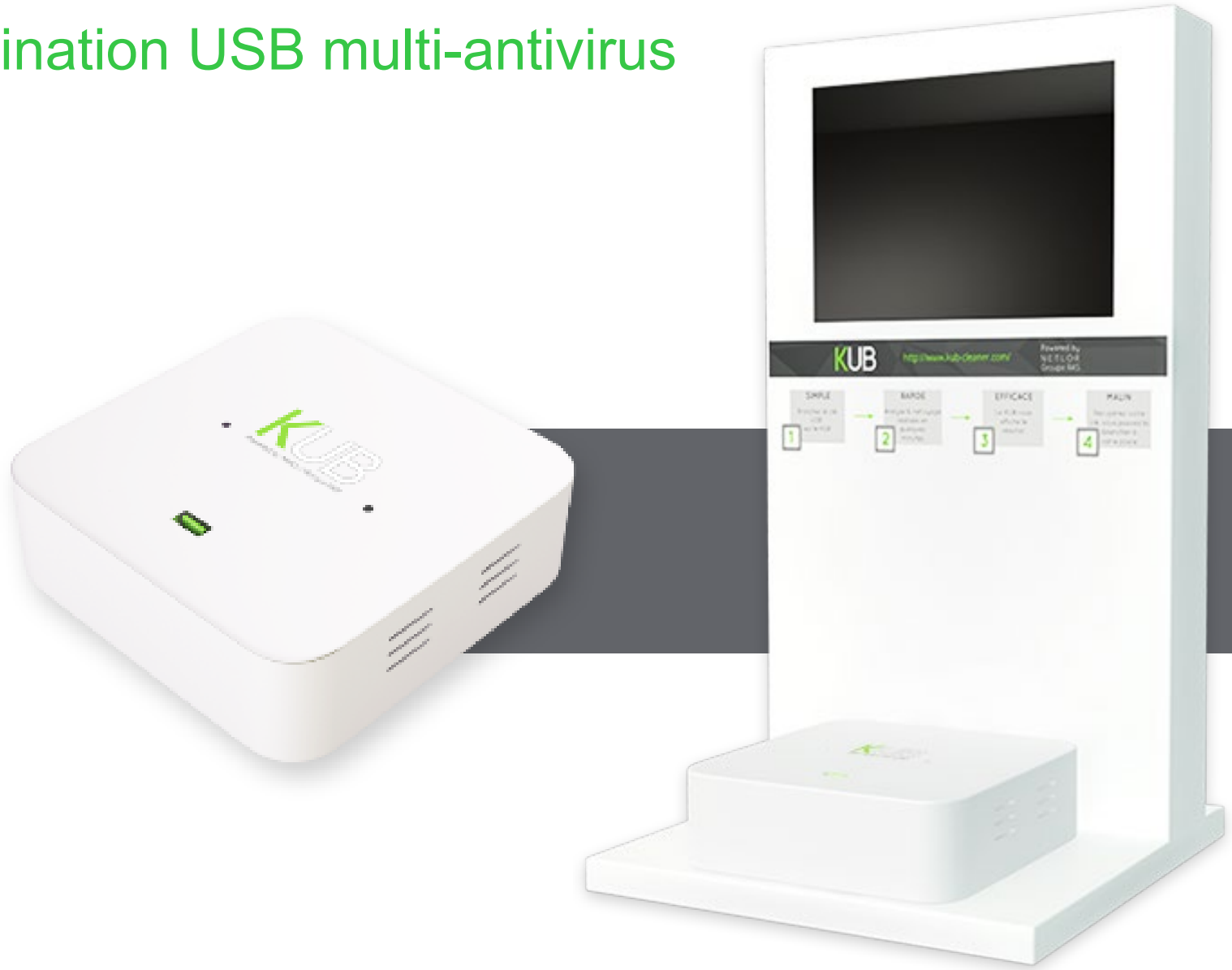
SOPHOS

F-Secure

eset ENJOY SAFER TECHNOLOGY™

KASPERSKY lab Internet Security

ClamAV



Life Is On Schneider Electric

Station de décontamination USB multi-antivirus

- La station KUB est une solution d'analyse et de décontamination des supports amovibles USB
- Cette solution participe à la protection des risques de corruption et de perte de données, d'arrêt de production ou de modification du comportement d'un SI Industriel

- ANSSI - La cybersécurité des systèmes industriels - Mesures Détaillées V1.0 2014 :

4.3.3 Interfaces de connexion

Références

Vulnérabilité : 2.2.3
Guide SCADA : BP03
Guide d'hygiène : Règles 5, 15 et 34
ISO 27002 : 12.6

Gestion des médias amovibles

Classe 1

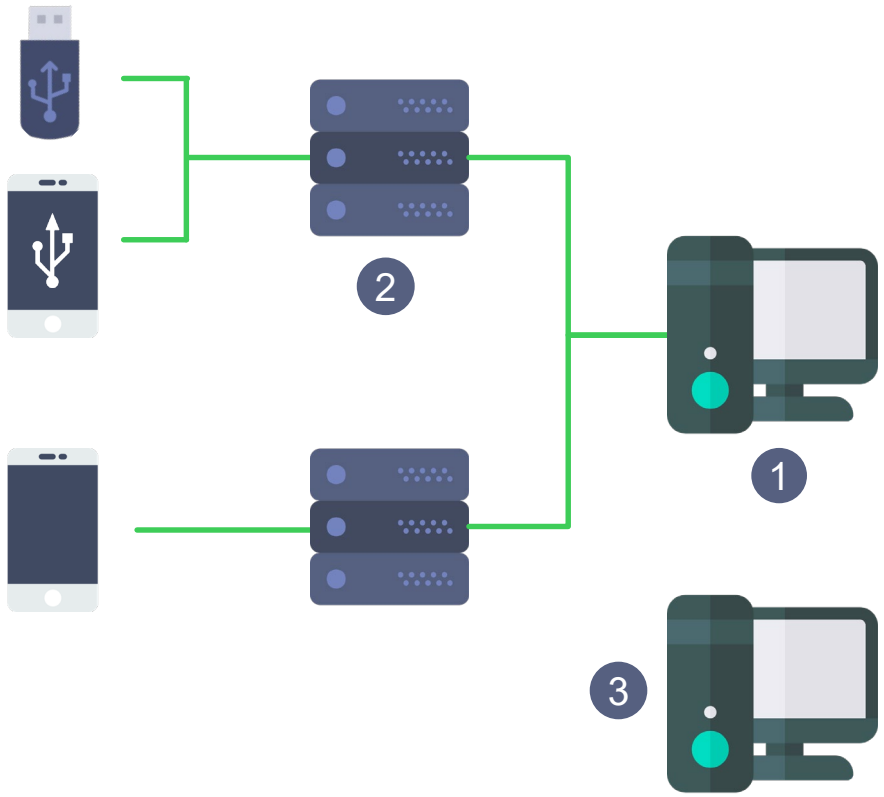
[R.233] Une politique d'utilisation des médias amovibles (clé USB, disquette, disque dur, etc.) devrait être définie.

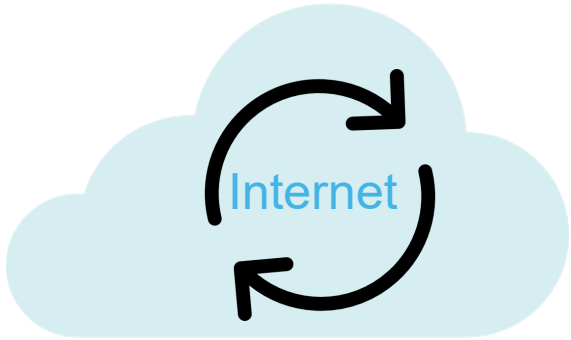
[R.235] Une station de décontamination devrait être installée afin d'analyser et décontaminer tous les périphériques amovibles avant de les utiliser sur le système industriel.

Classe 2

[D.238] Les recommandations R.233, R.234, R.235, R.236 et R.237 deviennent des directives.

Station de décontamination USB multi-antivirus





Solution en cours de certification ANSSI (CSPN)

Serveur KUB

SOPHOS
F-Secure
eset ENJOY SAFER TECHNOLOGY
KASPERSKY lab Internet Security
ClamAV

1 Serveur d'administration

- Virtual appliance
- Téléchargement et déploiement des mises à jour
- Paramétrage des stations (réseau, texte affiché…)
- Reporting

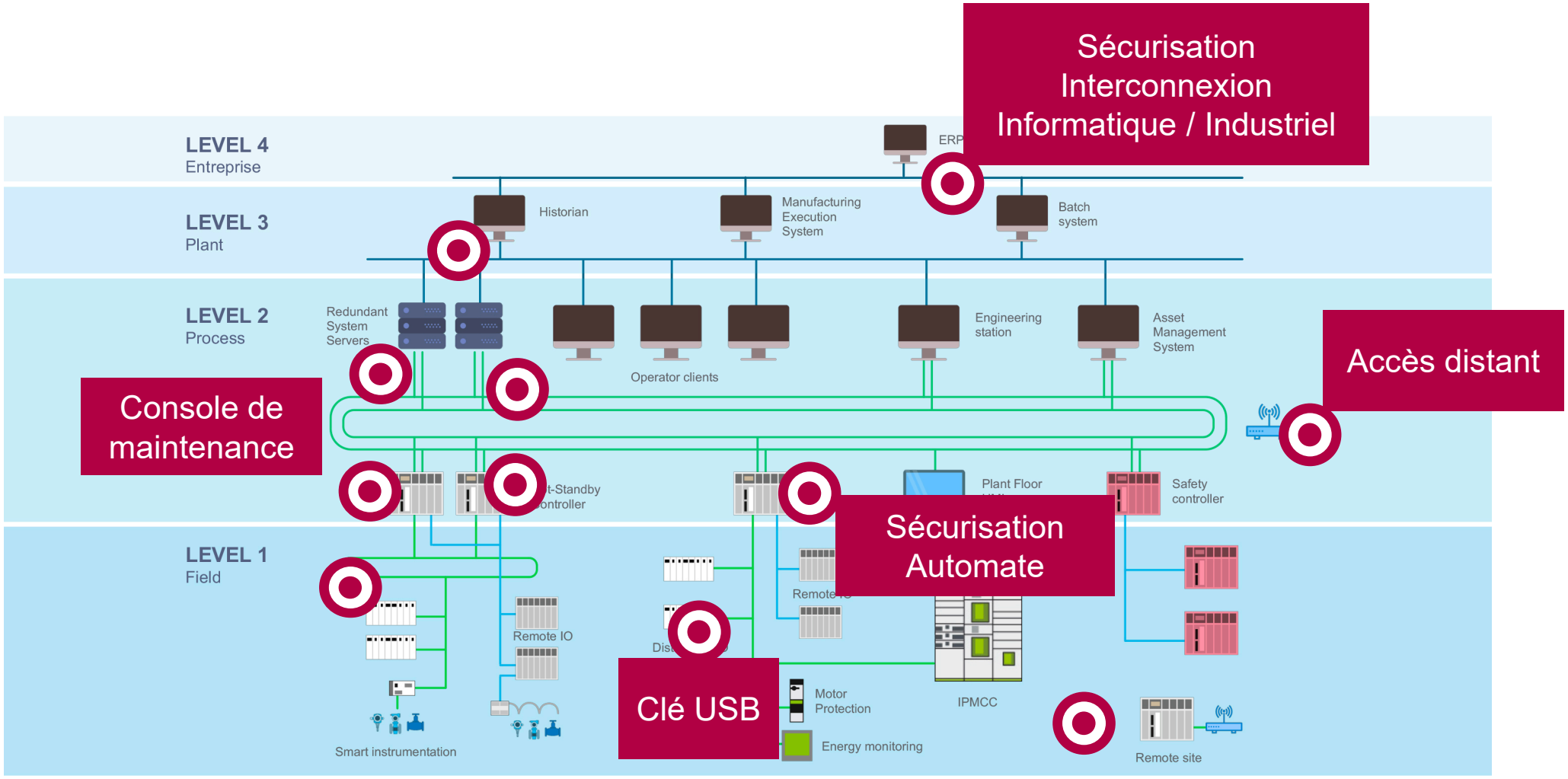
2 Station de décontamination

- Communication sécurisée avec le serveur (SSL)
- Possibilité d'installation sans réseau
- Scan automatique ou sur action utilisateur
- Nettoyage

3 Agent Workstation Protect

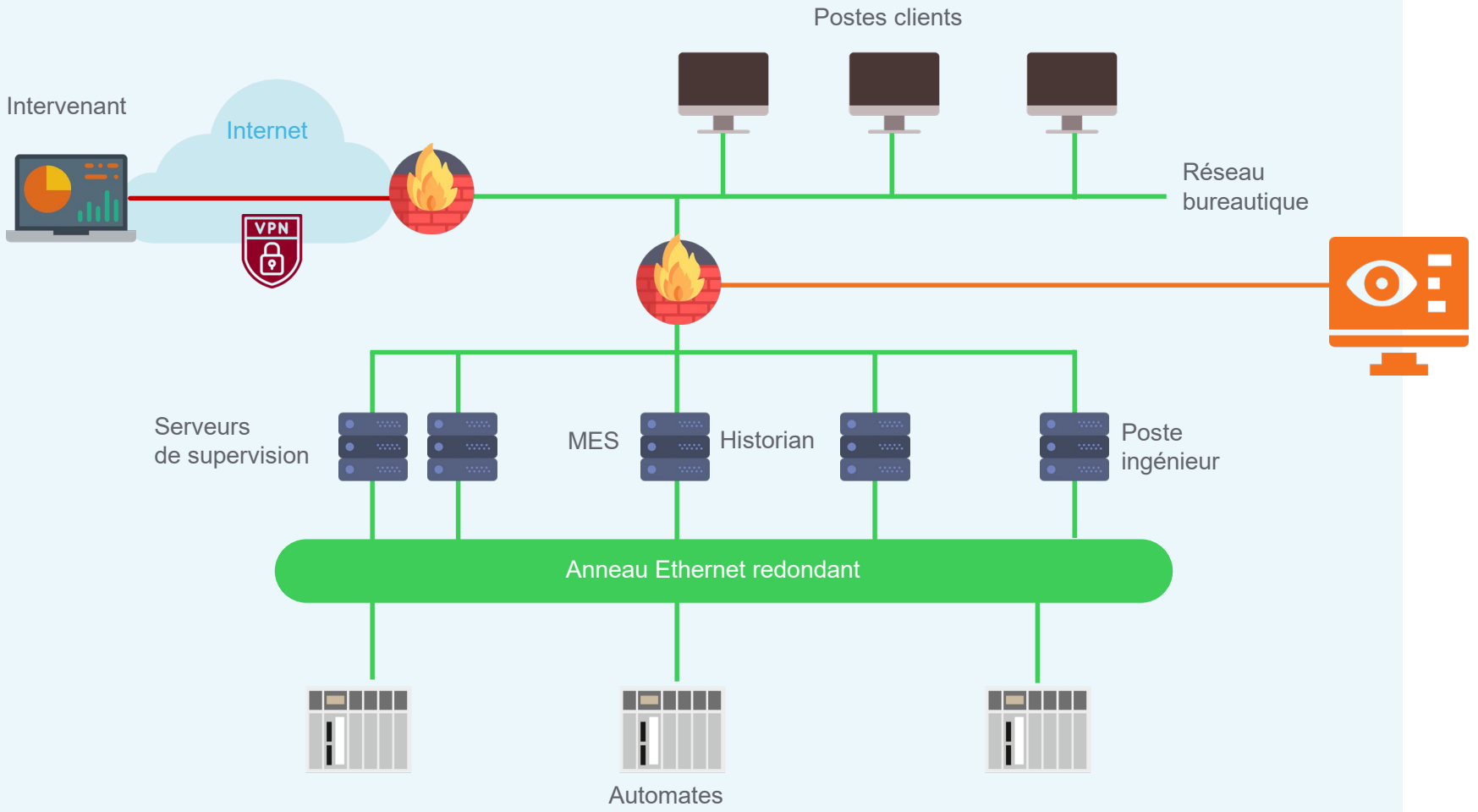
- Protection contre l'insertion de média non analysé
- Agent validé **à partir de Win XP SP2**
- Connecté ou non au serveur d'administration

Principaux vecteurs d’intrusion



niveaux selon le modèle ISA95

La télémaintenance sécurisée



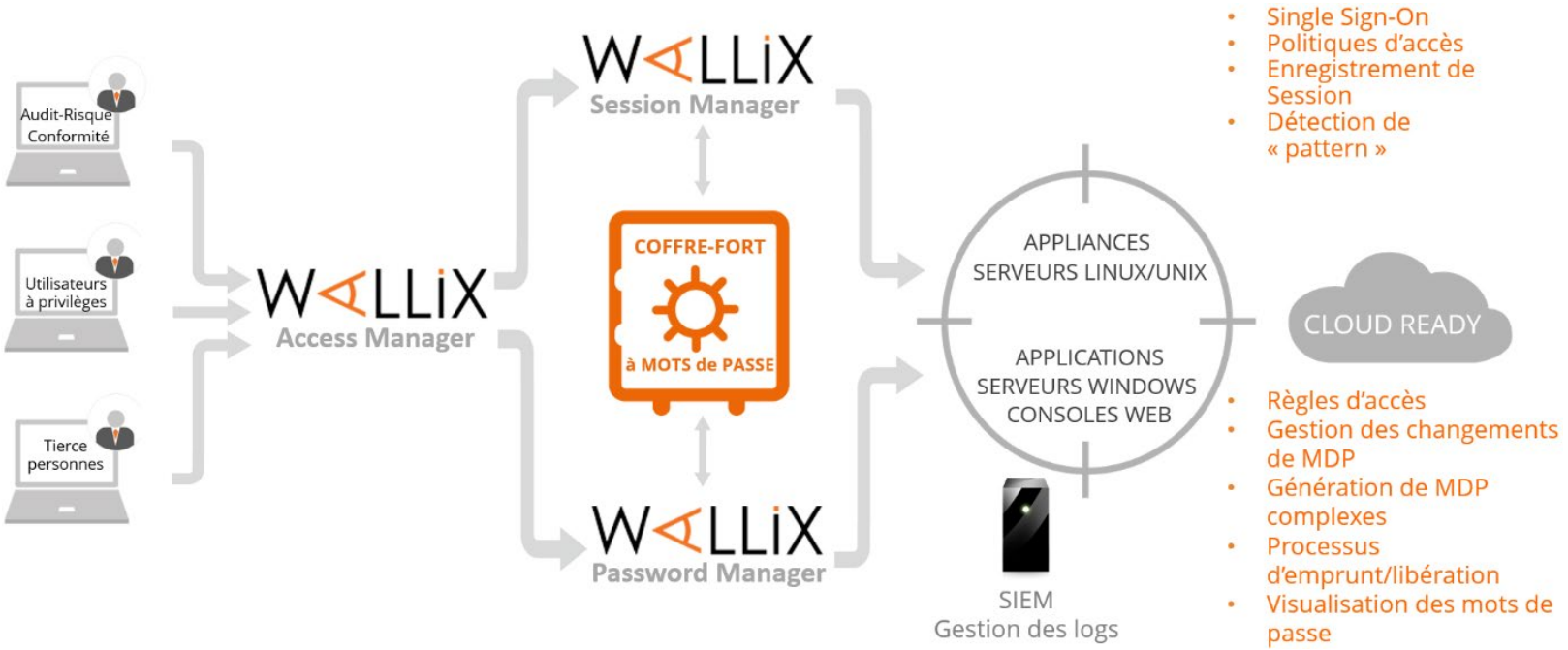
WALLIX
TRACE, AUDIT & TRUST

Traçabilité

Contrôle d'accès

Contrôle des actions

La télémaintenance sécurisée



- Architecture simple scalable et adaptable à toute situation (sites distribués, redondance active-active, active-passive…)
- Déploiement sans agent
- Intégration facile dans un environnement existant (virtuel, cloud, Active Directory, NTP, monitoring, syslog, SSO…)
- Gestion des changements de mots de passe (Windows, Linux, Oracle, MySQL, Cisco, Fortinet, Palo Alto…)

Formation à la Cybersécurité industrielle CYBINDUS

La formation débute par des rappels sur les systèmes industriels et la cybersécurité. Elle aborde ensuite les recommandations de l'ANSSI tant sur les aspects organisationnels que techniques. (Concepts, normes, méthodes, bonnes pratiques) Pour illustrer chaque thématique abordée, des exercices pratiques sont proposés soit sur table (Etude de cas pour la cartographie, l'analyse des risques) ou sur plateforme (VPN, firewall, automate).

Module de 3 jours
40% de Travaux Pratiques
Formation labellisée par l'ANSSI

SecNumedu
Formation continue
ANSSI


AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Attestation de conformité au référentiel SecNum*edu*-Formation Continue
visant à labelliser les formations continues en sécurité du numérique
attribuée à :
SCHNEIDER ELECTRIC France

Pour la formation continue
« *Cybersécurité des systèmes industriels* »

Référence de l'attestation : ANSSI-18-009
Valide jusqu'en août 2021

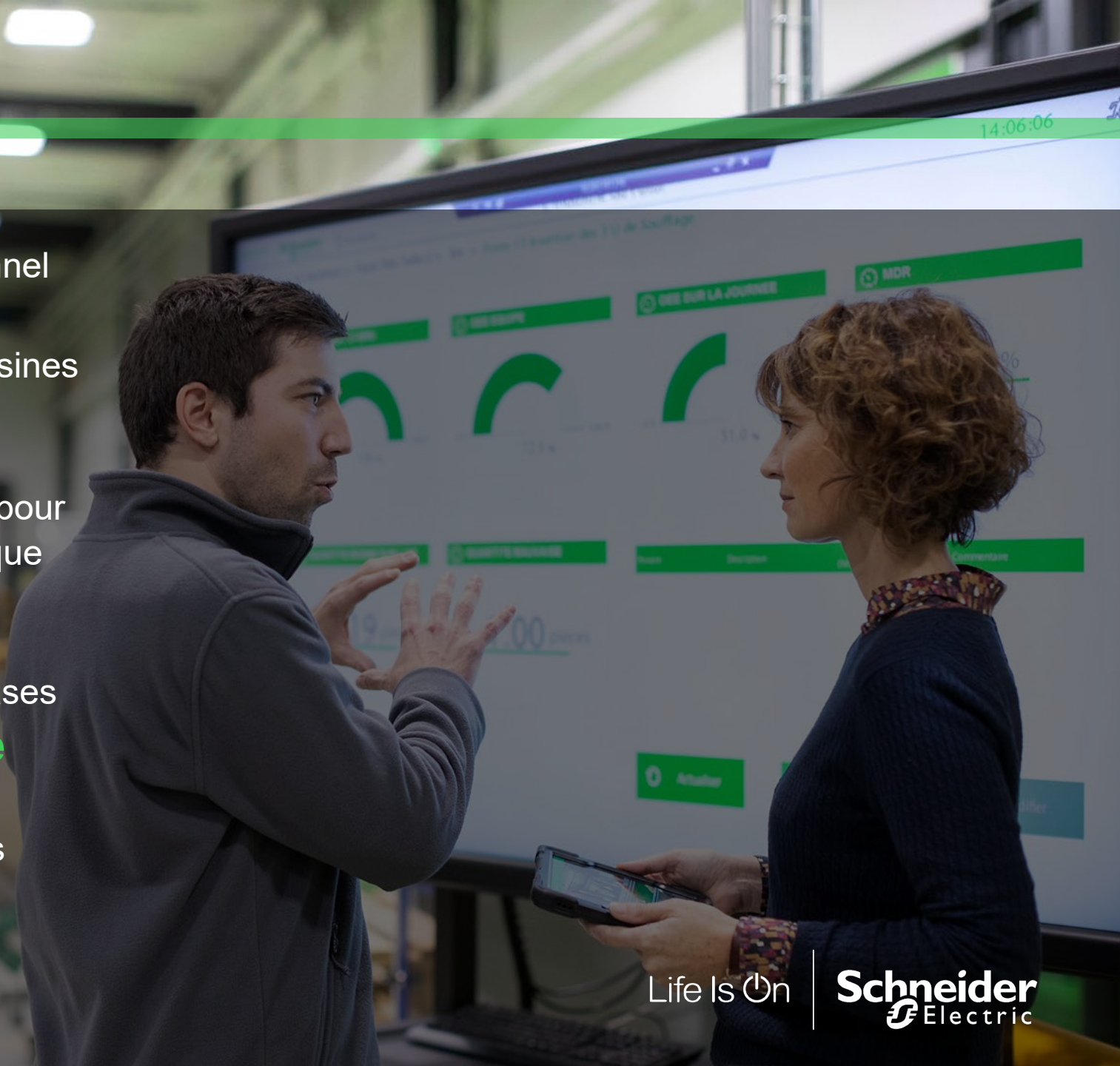
Paris, le 25/07/2019

Guillaume Poupard
Directeur général de l'Agence nationale de la sécurité des systèmes d'information

https://www.se.com/fr/fr/work/services/formation/industrie/cybindus.html

En conclusion

- **Sensibilisez** / **Formez** votre personnel
- **Evaluez** le niveau d'exposition de vos usines aux risques Cyber
- Définissez votre **architecture cible** pour traiter le risque à couvrir et acceptez le risque résiduel
- **Implémentez** en une ou plusieurs phases avec un **prestataire de confiance**
- **Maintenez** le niveau de sécurité de vos installations



Life Is On Schneider Electric

Des questions ?

Yann BOURJAULT
Directeur France Transformation Digitale & Cybersécurité
@ Yann.bourjault@se.com
06 30 65 02 75

Life Is On Schneider Electric