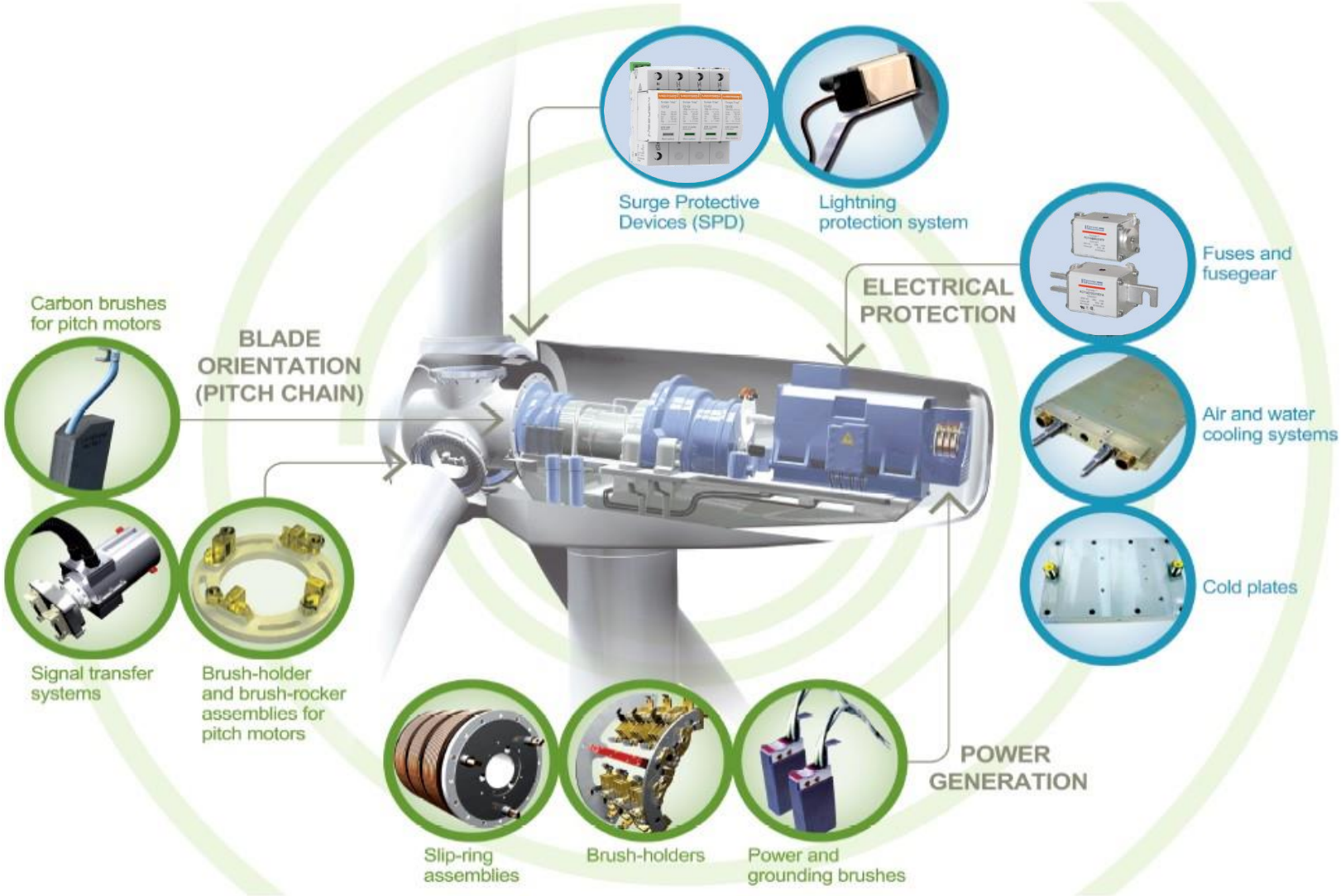
Sécurité des Systèmes d'Information

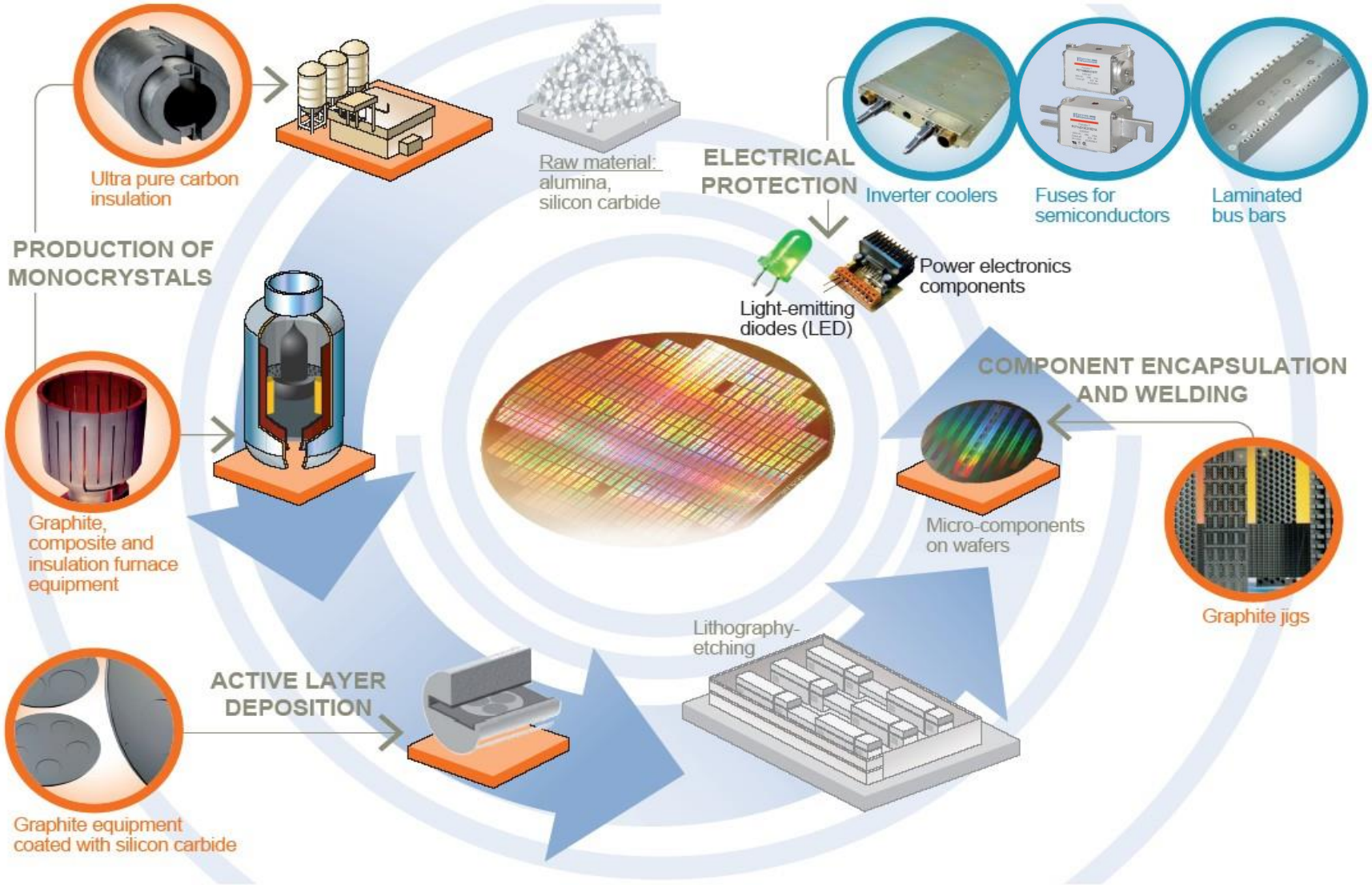
OSSIR

Janvier 2017

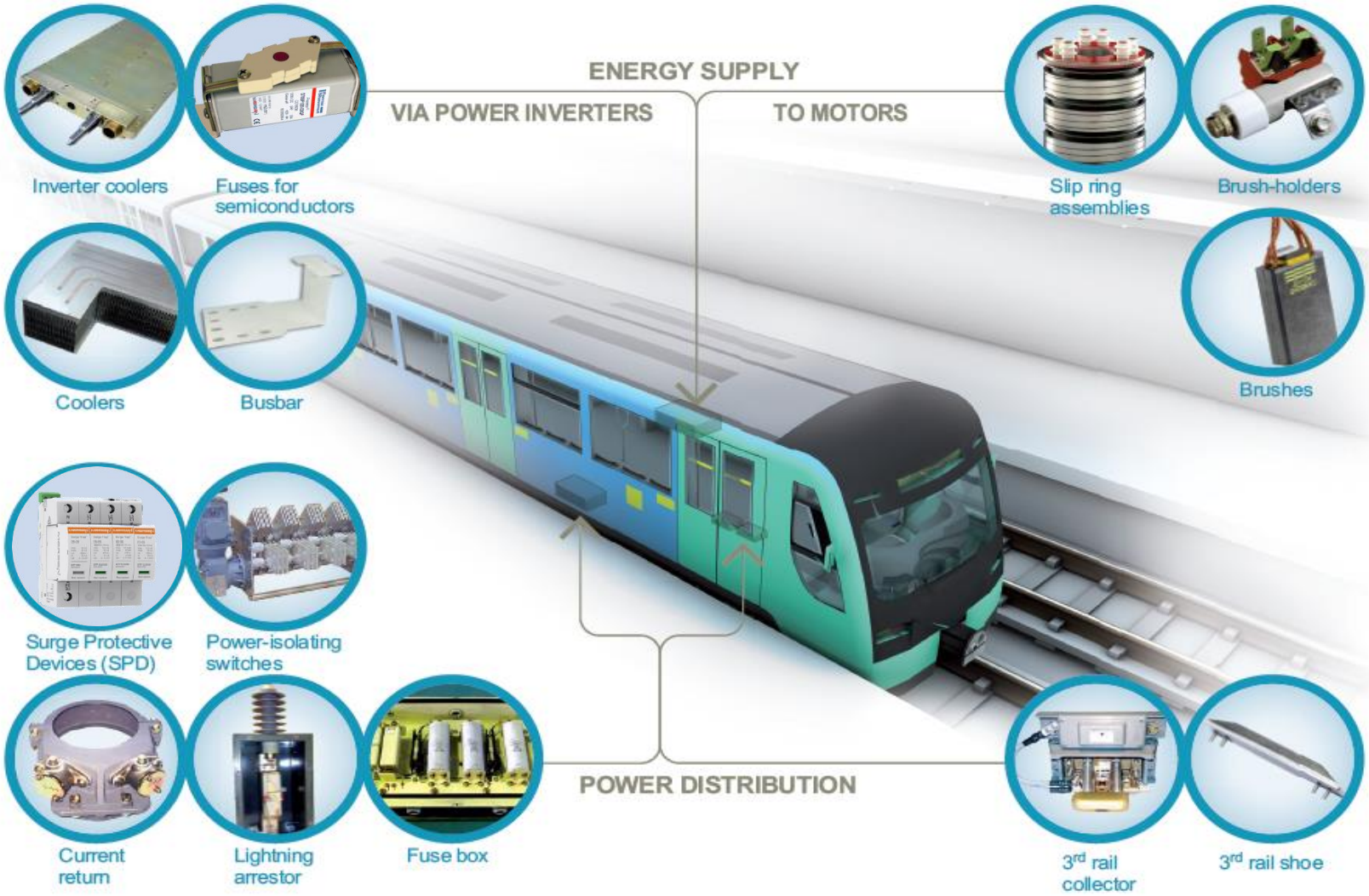
MERSEN DANS L'INDUSTRIE ÉOLIENNE



MERSEN DANS LE PROCÉDÉ DES SEMI-CONDUCTEURS



MERSEN DANS L'ÉQUIPEMENT FERROVIAIRE



2015 Key figures

Sales

€772M

- 37% Americas
- 34% Europe
- 29% Asia & other

EBITDA Margin

12,7% of sales

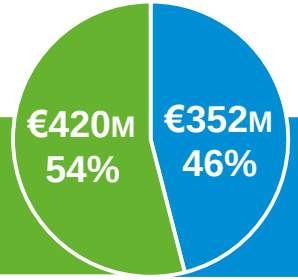
- Possibility of investing to maintain our leadership positions

Employees

6,375

- 35 countries of location

OUR EXPERTISE



ADVANCED MATERIALS

ANTICORROSION EQUIPMENT

GRAPHITE SPECIALTIES

POWER TRANSFER TECHNOLOGIES

ELECTRICAL POWER

ELECTRICAL PROTECTION & CONTROL

SOLUTIONS FOR POWER MANAGEMENT

APPROX. 25% MARKET SHARES WITH LEADING POSITION WORLDWIDE

New Group segment organization as of January 2016 – 2015 sales figures

Forces et faiblesses impactant les SI

- **Des problématiques de groupe international avec des structures locales de PME**

  - Des écueils à contourner
    - La masse critique pour traiter avec les grands acteurs de l'informatique est parfois insuffisante
    - Des ressources informatiques quantitativement réduites, surtout sur les « petits » sites
    - Une dispersion géographique et linguistique incontournable
    - Des produits et procédés multiples

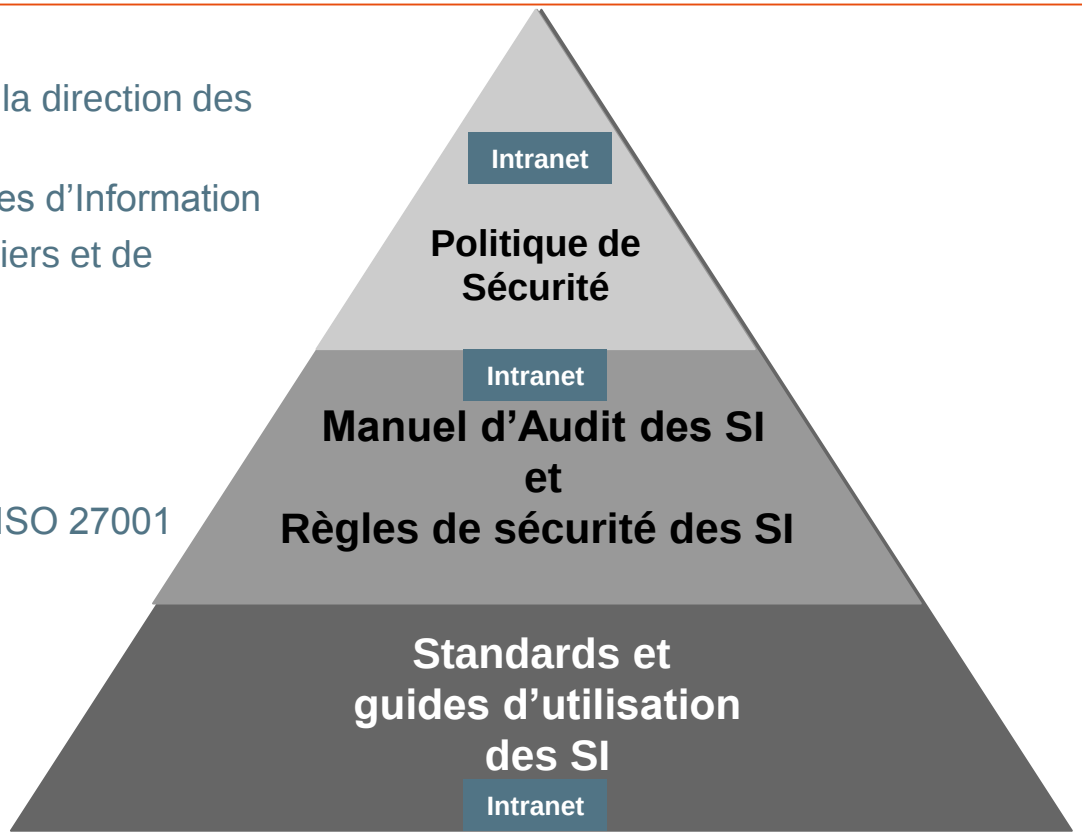
  - Des atouts
    - Une taille humaine qui facilite la communication
    - Peu de niveaux hiérarchiques
    - Faible turnover des équipes
    - Une forte culture de la sécurité
    - Des équipes motivées et consciencieuses

Quelques chiffres sur les systèmes d'Information

- **35 Pays**
  - Pays industrialisés et zones urbaines
- **75 Sites**
  - De 5 à 400 PCs
- **4000 Pcs**
  - Un master unique pour tous, déployé par Dell en usine
- **400 Serveurs**
- **Environ 80 Personnes impliquées dans les systèmes d'information, incluant des « non informaticiens »**

UNE POLITIQUE DE SÉCURITÉ FORMALISÉE DES SYSTÈMES D'INFORMATION

- Dépend du DSI avec un lien fonctionnel « fort » de la direction des l'audit et des risques
- Relève sur les sites du Correspondant des Systèmes d'Information
- Relayée si besoin par les coordinateurs SI des métiers et de régions
- Publiée dans l'Intranet
- Diffusée par mail aux correspondants
- Promue par une formation en ligne
- Inspirée des règles de l'hygiène de l'ANSSI et de l'ISO 27001



Notre objectif est d'obtenir un niveau de sécurité raisonnable sur un spectre le plus large possible, avec une bonne acceptation de nos utilisateurs

Infrastructure : centralisation des principaux centres de données

- **Une rationalisation progressive**
  - 2005:
    - 25 ERP
    - 22 messageries
    - Pas de constructeur mondial de PC
  - 2015:
    - Une solution unique d'ERP
    - 4 centres de données
    - Une seule solution de messagerie
    - Un master unique sur tous les sites
    - Une gestion unique des terminaux mobiles
    - Un réseau professionnel indépendant et protégé d'Internet
- **Gain = diminution de la surface d'attaque, augmentation de la qualité et de la maîtrise des solutions**

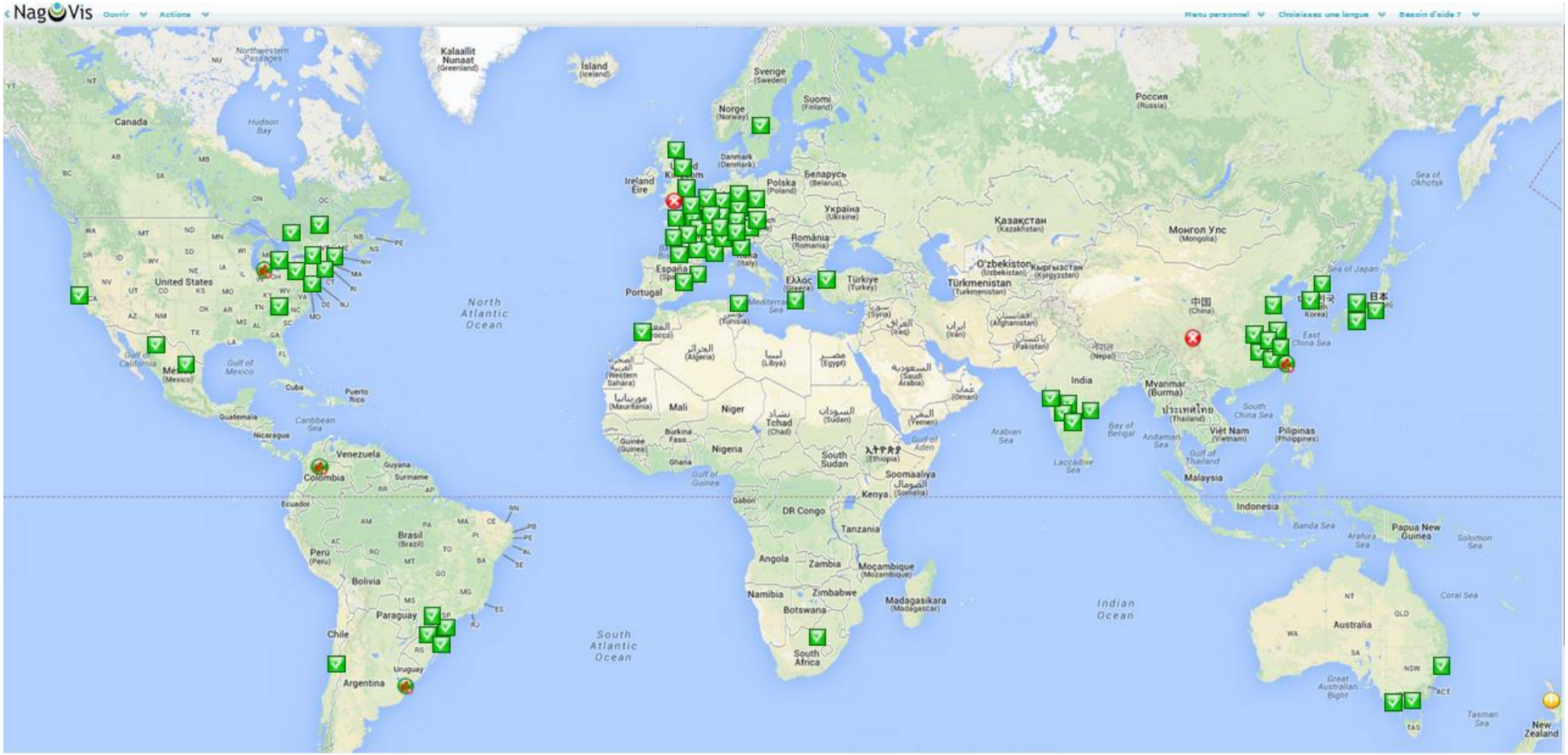
Les éléments de protection - 1

- **Cartographie des risques**
  - Elle a été effectuée cette année sous un angle « métier »
  - Elle sera mise à jour annuellement (tous les trois ans auparavant)

- **Une surveillance en temps réel de nos centres de données, avec une centralisation des solutions et des consoles**
  - Antivirus
  - Antispam
  - Messagerie
  - Navigation
  - Solution de mobilité unique (MDM)
  - Télécoms (routage, priorisation des flux)
  - Anti-intrusion etc.
  - Les consoles sont un excellent moyen de faire prendre conscience des risques aux utilisateurs.

SUPERVISION DES SITES EN TEMPS REEL

- Carte en temps réel des sites, connectivité réseau → réactivité, transparence



Les éléments de protection - 2

- **Diminution de la surface d'attaque**
  - Exemple du master: un master unique, élaboré en collaboration avec les sites: expression des besoins, et surtout, des tests.
  - La sécurité est prise en compte dès l'élaboration du master avec la suppression de certaines applications et services inutiles, avec des réglages de sécurité appropriés
  - Les applications Groupe sont vérifiées et testées sous l'angle de la sécurité dès la conception, dans la mesure du possible. L'intervention a lieu dès le cahier des charges.

- **Défense en profondeur**
  - L'objectif est de ne pas exposer les utilisateurs et services directement sur Internet mais au travers de différentes couches de protection différentes
  - Filtrage URL Globalisé
  - Antivirus de navigation Web différent de l'antivirus des PC/serveurs
  - L'option de sandboxing sur l'antispam donne d'excellents résultats

- **Une procédure spéciale d'intégration des nouveaux sites et joint ventures**

Les éléments de protection - 3

- **Des audits informatiques à distance**
  - Plusieurs sites par mois:
    - Tous les sites « importants » sont testés annuellement
    - Les sites qui vont faire l'objet d'un audit Groupe en local sont testés en avance de phase
    - Des tests peuvent être effectués sur demande du site
  - Tests de vulnérabilité simples et faits de l'intérieur
  - Vérification de conformité et de qualité à l'aide des consoles de supervision
- **Audits groupe généraux**
  - Lors des audits Groupe, l'informatique est vérifiée, suivant le manuel d'audit et les résultats de l'audit à distance et les résultats de l'analyse de risques
  - Les entretiens avec les équipes sont riches en information
- **Audits externes**
  - Des études périmétriques pour vérifier que tous nos points d'accès sont connus
  - Des audits de la politique de sécurité
  - Réunions d'échange avec des sociétés comparables à Mersen

Les éléments de protection - 4

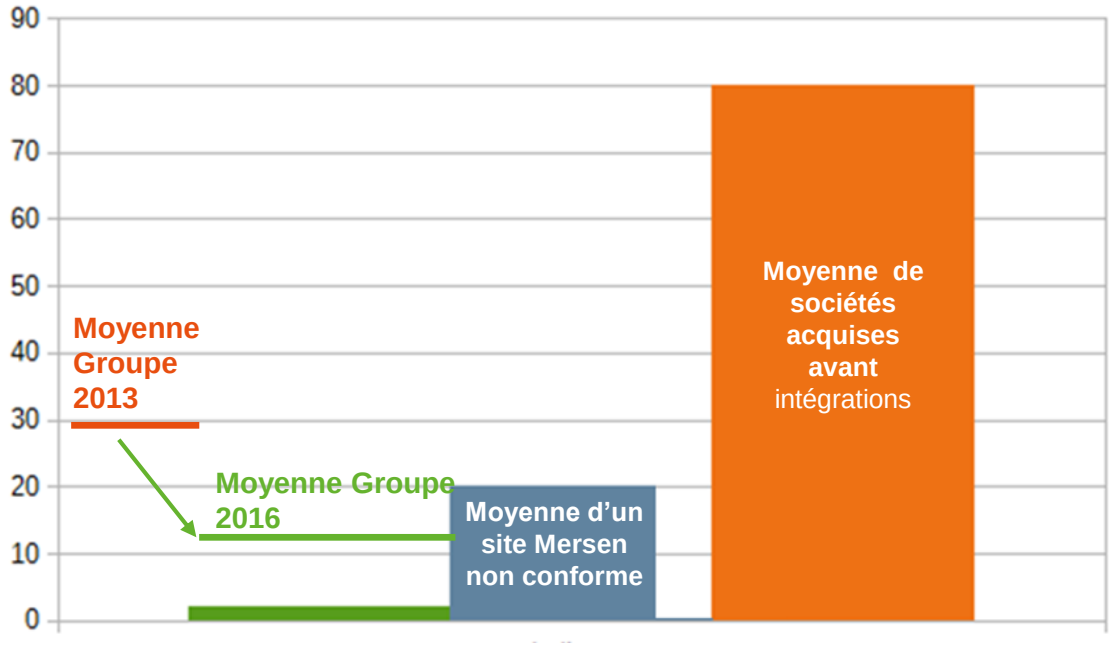
- **Cyber-surveillance (externe)**
  - Des fuites de données ont elles lieu et des éléments Mersen se retrouvent ils dans le Darknet?
  - Les points d'entrée du réseau sont ils sécurisés et à jour ?

- **Communication**
  - Liste de diffusions aux Correspondants SI et Correspondants Systèmes Industriels
  - Toutes les notices d'installation, et les instructions de sécurité sont disponibles sur l'intranet.
  - La documentations est multi-langues dès qu'il s'agit de s'adresser aux utilisateurs
  - Formation en ligne (Anglais, Français, Chinois)
  - Communication par l'exemple: déployer une solution de sécurité après une expérience réussie sur un site pilote, en plus du siège social et de la DSI

- **Facteur de succès**
  - Exemplarité de l'encadrement, des organes de direction et des informaticiens
  - Dialogue avec les utilisateurs: les équipes sont très consciencieuses et motivées, il faut expliquer en quoi la sécurité des SI les concerne: parfois un simple questionnement suffit pour illustrer et convaincre.

Un indicateur clé suivi pour tous les sites mensuellement

- Cet indicateur est basé sur le pourcentage mensuel de PC en contact avec au moins une menace
- Si la défense en profondeur est efficace, la diminution de la surface d'attaque effective et les règles suivies, cet indicateur doit être très bas
- Il donne une bonne idée du niveau de conformité d'un site par rapport aux autres (benchmarking)
- La moyenne Groupe s'est améliorée en passant de 20% à 4% en quatre ans, suite à des améliorations locales et des modifications d'infrastructures
- Deux exemples: Une usine en Inde / une découpeuse jet d'eau en Europe



Sécurité des Systèmes Industriels

Contexte

- La première étude a été effectuée en 2004
- La mise en place d'une politique dédiée a été décidée en 2013
- Mersen ayant une large gamme de produits, les systèmes industriels sont très diversifiés: type, âge, fabricant, cahier des charges du client, compétences locales, proximité du fabricant …

Organisation basée sur un binôme:

- Correspondant Informatique local
- Responsable industriel: en général un responsable de maintenance industrielle
- Le binôme met à jour annuellement la liste du matériel
- Le responsable industriel évalue les risques associés au matériel
- Ces responsables industriels sont dans la liste de diffusion des informaticiens

Des bonnes pratiques adaptées à Mersen

- Basées sur le paramétrage du master et les bonnes pratiques SI du Groupe
- Basées sur les recommandations de l'ANSSI

Et, surtout

- Expliquer aux équipes industrielles le but recherché par les informaticiens
- Comprendre le but recherché par les techniciens

Les axes d'amélioration décidés

- Augmenter les contacts avec des sociétés équivalentes
- Plus de communication dirigée vers les utilisateurs
- Exploiter les alertes de nos consoles de supervision d'une façon périodique et plus fine

Mersen

Expertise, our source of energy