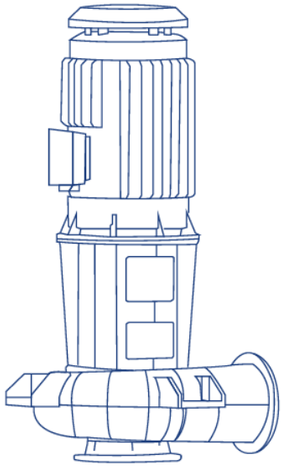


SNECOREP®

LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

Les matinées thématiques

Sofrel LACROIX

CHESTERTON®

SNECOREP

LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

- **LACROIX SOFREL - 1h / 10h – 11h**
  - Samuel Espinasse
  - Ludovic Pertuisel
- **ASTEE - 10 min**
  - Alexander Foote
- **CHESTERTON – 1h / 11h – 12h**
  - Laurent Sant
  - Laurent Prunier Duparge
- **Cocktail déjeunatoire – à partir de 12h15 – Au rez de chaussée – salle habituelle.**

Sofrel LACROIX

CHESTERTON

Téléchargez l'application

Télécharger dans l'App Store

DISPONIBLE SUR Google Play

LACROIX

MATINALE DU 20 MAI 2026

LA CYBERSECURITE: DEFIS REGLEMENTAIRES & ORGANISATIONNELS POUR LES EXPLOITANTS DES RESEAUX D'EAU

Une ETI technologique & industrielle **française** à la dimension **internationale**

445M€
Chiffre d'affaires 2025

2 850
Collaborateurs

Répartis dans
10 pays

Groupe familial côté
sur Euronext depuis 1992

62%
du capital détenu par
la famille BEDOUIN

IMPLANTATIONS

EMEA

- FRANCE
- ALLEMAGNE
- ESPAGNE
- ITALIE
- POLOGNE
- TUNISIE
- BELGIQUE
- ARABIE SAOUDITE

APAC

- SINGAPOUR
- CHINE

Notre **mission**

Fournir à nos clients des **équipements électroniques** et des **solutions IoT industrielles fiables et sécurisés** pour leurs applications critiques

Activité Electronics

Accompagner nos clients de la conception à la fabrication de l'électronique embarquée dans leurs solutions

304M€

Activité Environment

Accompagner nos clients publics et privés dans l'optimisation et la sécurisation de la gestion des réseaux d'infrastructures critiques

141M€

POUR LES LEADERS TECHNOLOGIQUES & INDUSTRIELS

CAC40 – NEXT40
ETI & équivalents internationaux

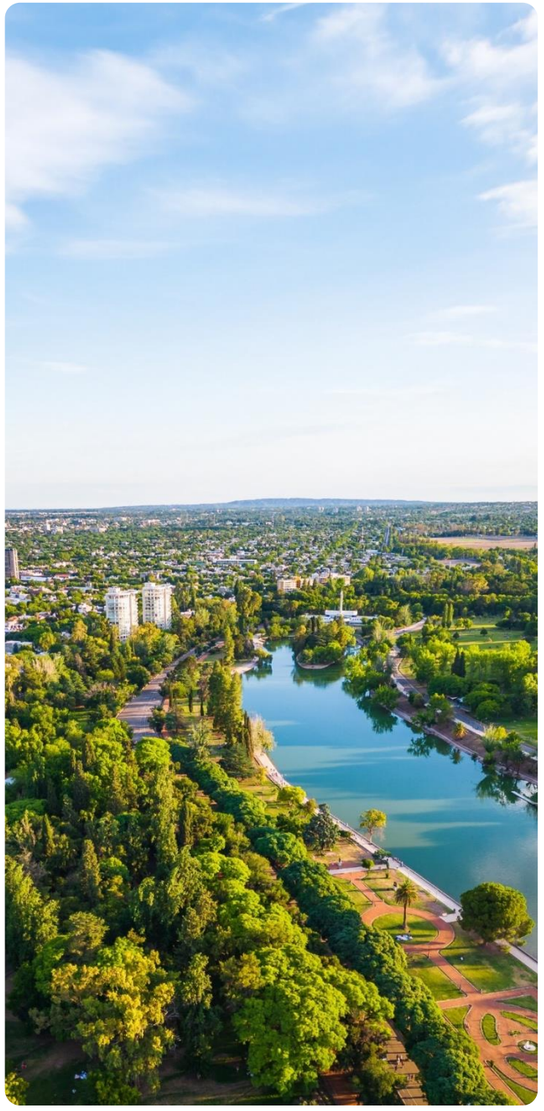
- Automobile
- Industrie
- HBAS (Maisons & bâtiments connectés)
- Aéronautique & défense
- Santé

POUR LES EXPLOITANTS DES INFRASTRUCTURES D'EAU & D'ÉNERGIE

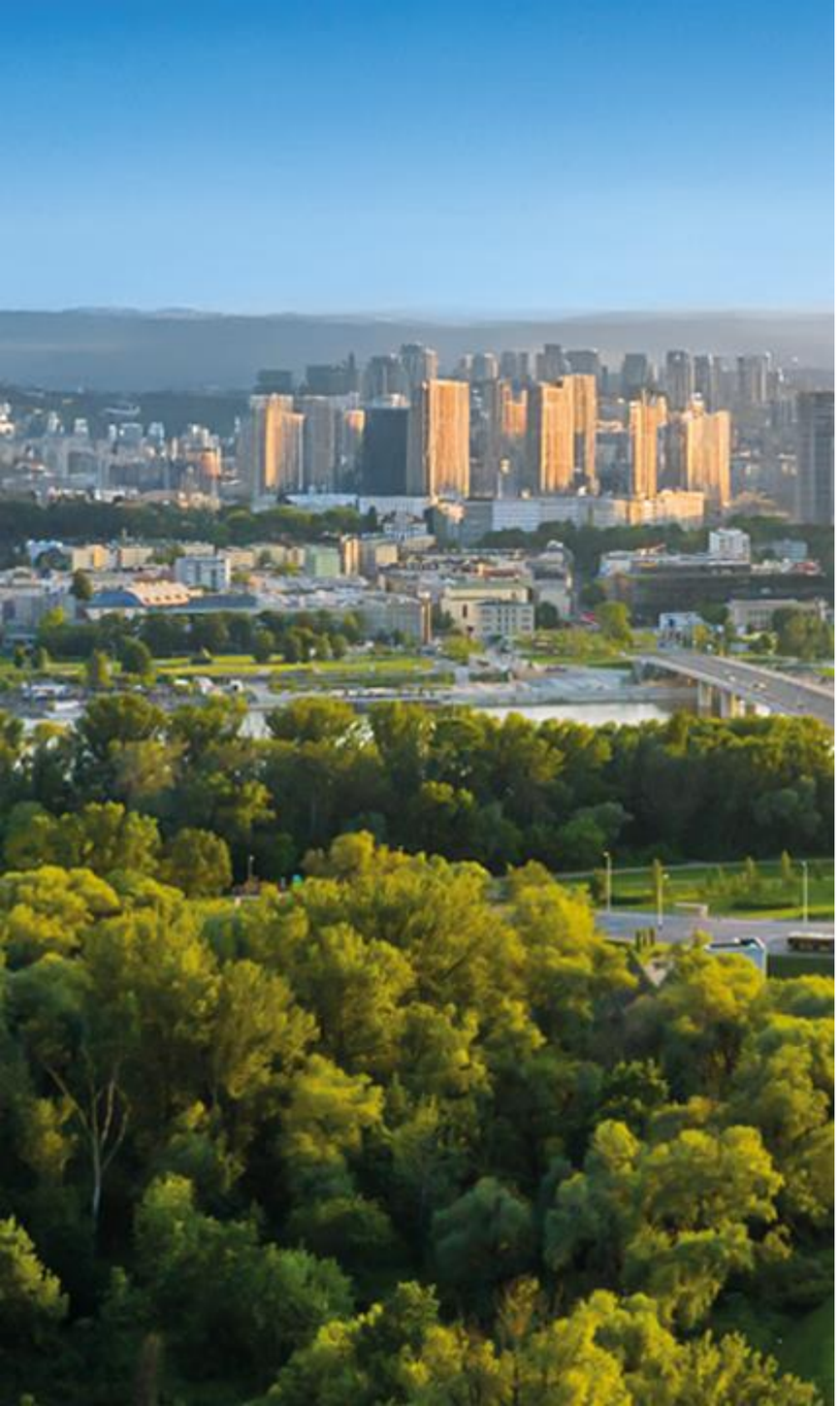
Exploitants – Intégrateurs & installateurs - Bureaux d'études – Industriels
Collectivités locales - Syndicats intercommunaux – Bailleurs sociaux

- Réseaux d'eau
- HVAC (Chauffage, Ventilation, Climatisation)
- Smart grids (Réseaux électriques)
- Eclairage public

Nos 4 engagements pour une **électronique utile** & **durable**



	INDICATEURS D'IMPACT	2024	2024 Sans ELEC NA	OBJECTIFS
DÉVELOPPER NOS ACTIVITÉS À IMPACT POSITIF	Part de produits à impact dans le CA	67%	71%	80% en 2030
CONCEVOIR DES SOLUTIONS ECO-EFFICIENTES	Part de nouveaux produits LACROIX écoconçus	71%	71%	100% en 2025
CONDUIRE NOS OPÉRATIONS DE MANIÈRE DURABLE	Emissions de GES scopes 1&2 ($KtCO_2e$)	11	9,2	5,8 en 2033 (-55% vs 2023)
	Emissions de GES scope 3 (tCO_2e/K€ VA)	15,7	13,3	6,9 en 2033 (-61% vs 2023)
	Déchets générés (kg/K€ de CA)	2,8	2,3	2 en 2030
	Part de volume d'achat couvert par une évaluation RSE	En cours	En cours	75% en 2025
S'ENGAGER POUR NOS ÉQUIPES & NOS TERRITOIRES	Sites LACROIX labellisés Great Place to Work	53%	62%	100% en 2030
	Femmes parmi les managers	35%	36%	40% en 2030



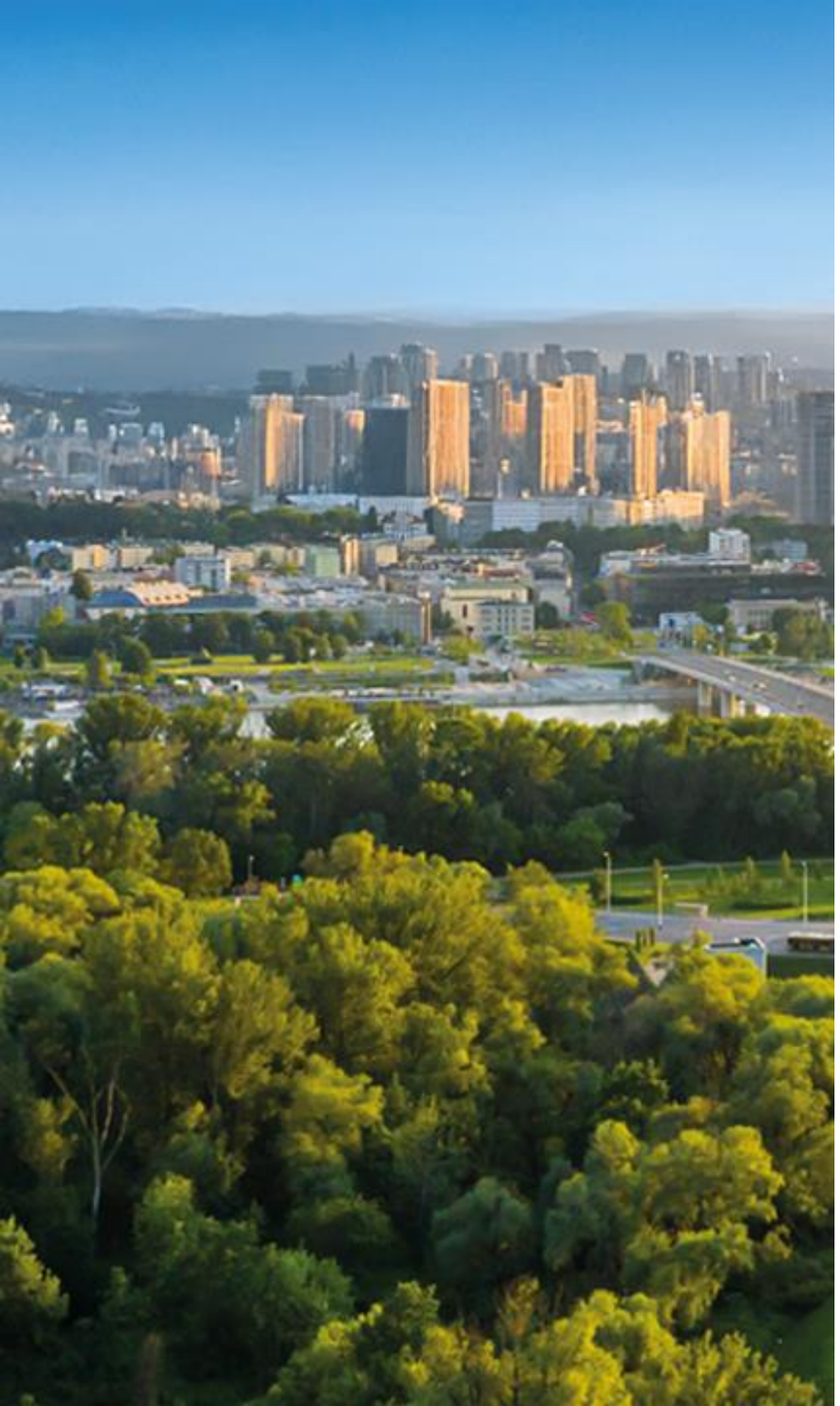
AGENDA

01 Cybersécurité dans l’eau, mythe ou réalité ?

02 Cybersécurité: Directive NIS2

03 Cybersécurité: Règlement CRA

04 Conclusion



AGENDA

01 Cybersécurité dans l’eau, mythe ou réalité ?

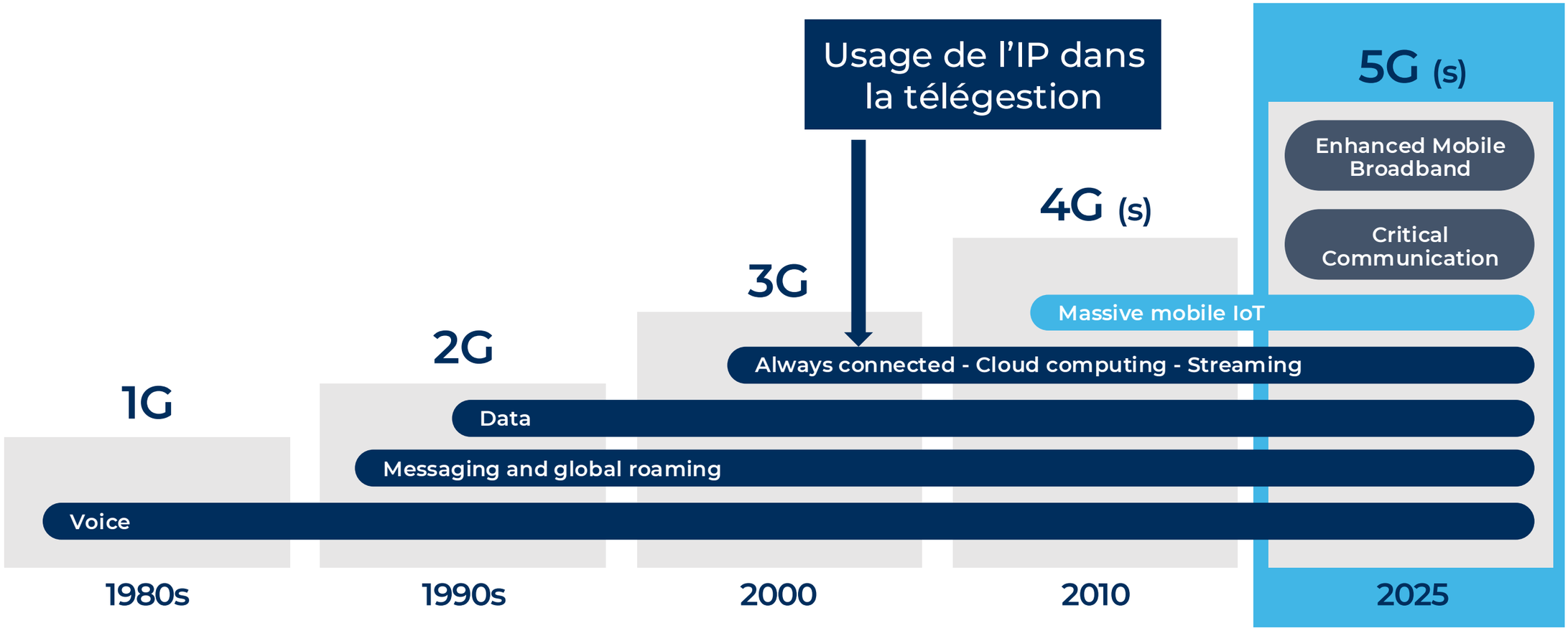
02 Cybersécurité: Directive NIS2

03 Cybersécurité: Règlement CRA

04 Conclusion

Régulation connectée : **une adaptation continue** nécessitant de la **cybersécurité**

Vers la 5G



L'utilisation de l'IP et d'Internet augmente la vulnérabilité des systèmes

Réalité de la menace

2025

Pologne

Plusieurs stations de traitement d'eau ont subi des intrusions dans leurs systèmes de contrôle industriel. Avec, dans certains cas, une capacité concrète de modifier les paramètres de procédé.

Rapport de l'agence de sécurité intérieure

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO
2024–2025

https://www.abw.gov.pl/pl/aktualnosci/2815,Agencja-Bezpieczenstwa-Wewnetrznego-2024-2025-Wybrane-aktywnosci.html

2024/2021

USA

OLDSMAR - L'intrus prend le contrôle sur le système central et modifie le point de consigne de l'hydroxyde de sodium (produit chimique utilisé pour le traitement des eaux pour réguler l'acidité de l'eau potable) du système de 100 parties par million (ppm) à 11 100 ppm. L'opérateur ramène l'hydroxyde de sodium à un niveau correct. La cyberattaque n'a eu aucun impact sur la qualité de l'eau.

Aliquippa - groupe iranien Cyber Av3ngers, accès à un automate Unitronics via **internet** avec **identifiants par défaut**

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

https://www.aria.developpement-durable.gouv.fr/accident/57579/

2023

Irlande

Comté de Mayo - groupe iranien Cyber Av3ngers, accès à un automate Unitronics via **internet** avec **identifiants par défaut.**
160 foyers coupés d'alimentation en EP **pendant 2 jours**

https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/

La cyber sécurité en France

Agence Nationale de la Sécurité des Systèmes d'Informations

Défendre

les systèmes d'information critiques de la Nation en concevant et opérant des capacités de détection des cyberattaques, et en garantissant la disponibilité de produits de sécurité de confiance capables de protéger les données les plus sensibles et de répondre aux menaces les plus élevées ;
les victimes de cyberattaques et la Nation, en structurant au niveau national l'assistance aux victimes ;
une vision autonome de la sécurité et de la stabilité du cyberespace au niveau international.

Connaître

l'état de l'art en sécurité des technologies et des systèmes d'information ;
les menaces et les risques dans le cyberespace ;
les tendances du monde de la cybersécurité, en France, en Europe et à l'international.

Partager

des recommandations, des méthodes et des outils aux acteurs de la cybersécurité et du numérique ;
de la connaissance et des savoir-faire sur la menace et les réponses possibles, avec les partenaires techniques, opérationnels et stratégiques, qu'ils soient français, européens ou extra-européens ;
largement son expertise pour renforcer la sécurité collective face aux risques cyber.

Accompagner

le déploiement d'une politique publique en matière de cybersécurité et sa déclinaison territoriale ;
les autorités dans leur compréhension du fait cyber ; les organisations régulées dans l'application des mesures de protection de leurs systèmes d'information et leurs réponses aux incidents ; la montée en compétence des administrations et du secteur privé par le développement des formations en cybersécurité ;
le développement d'un écosystème de prestataires privés de produits et de services de confiance.

Réguler

la qualité des produits et services de cybersécurité au travers de démarches de qualification et de certification ; la qualité des produits embarquant des éléments numériques en promouvant la sécurité par conception et par défaut ; par la conception de dispositifs normatifs et réglementaires aux niveaux national, européen et international ; par le contrôle de leur bonne application.

La cybersécurité, **une évolution permanente**

Des réseaux plus performants… mais aussi plus exposés

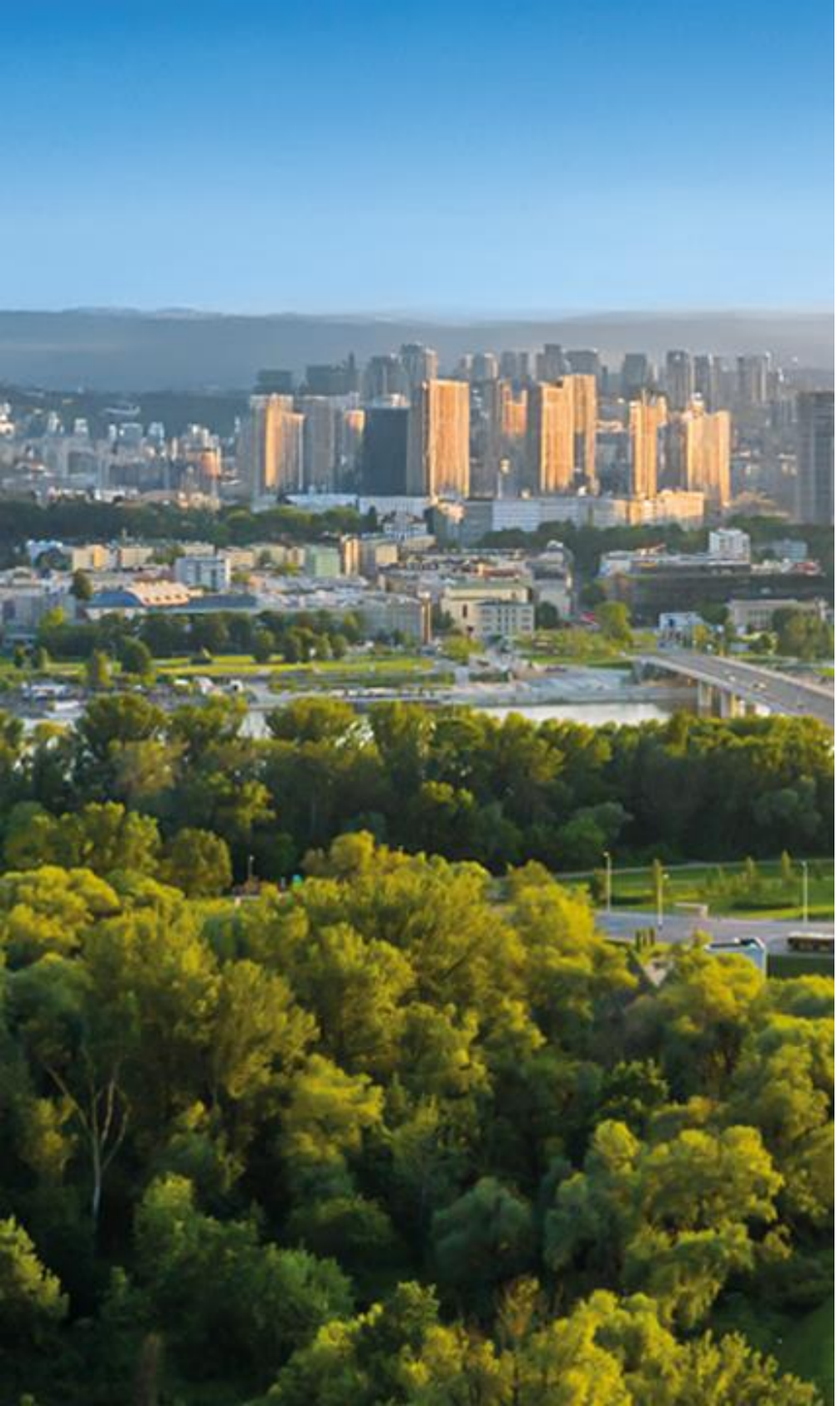
Depuis quelques années **les cyberattaques** visant les infrastructures critiques et les collectivités **se sont intensifiées**

La question n’est plus :

Est-ce que je vais être attaqué ?

Mais quand ?

Et de s’y préparer



AGENDA

01 Cybersécurité dans l’eau, mythe ou réalité ?

02 Cybersécurité: Directive NIS2

03 Cybersécurité: Règlement CRA

04 Conclusion

La cybersécurité, **une évolution permanente**

Législation

NIS2 Network & Information Systems Directive

CRA Cyber Resilience Act

Normes

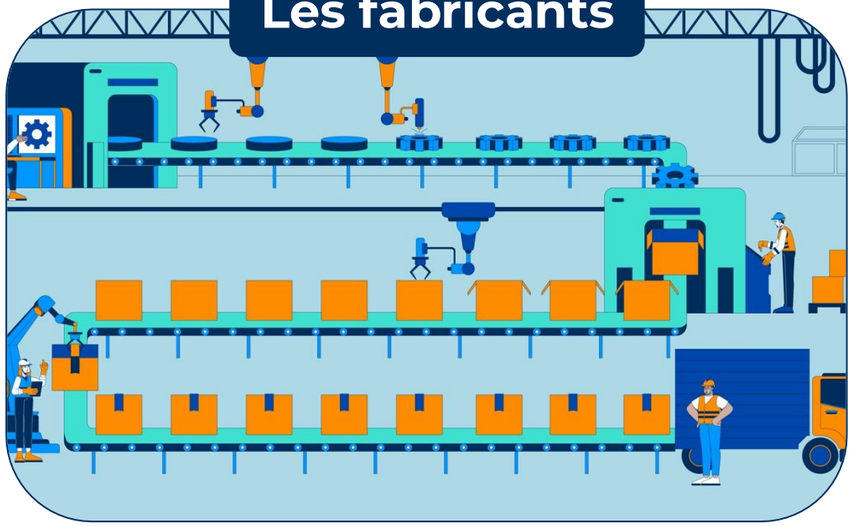
ISO 27001

IEC 62443

Qui est concerné ?

Les exploitants

Les fabricants



Renforcement du cadre réglementaire **européen**

Directive NIS2
(Network and Informations System Security 2)

Directive

Les directives sont des actes législatifs qui fixent des objectifs aux pays de l'UE. Toutefois, chaque pays est libre d'élaborer ses propres mesures pour les atteindre. La directive européenne sur les plastiques à usage unique en est un exemple. Elle réduit l'incidence de certains plastiques à usage unique sur l'environnement, notamment en réduisant, voire en interdisant, l'utilisation de plastiques à usage unique tels que les assiettes, les pailles et les gobelets pour boissons.

Cadre général

Définition des objectifs : sécurité, santé publique, environnement, qualité, interopérabilité… Définition des obligations générales (ce qu'il faut atteindre)

Sanctions & responsabilités

Amendes, restrictions d'exploitation, obligations de mise en conformité, responsabilités civiles ou pénales selon les cas.

Règlement Cyber Resilience

Règlement

Les règlements sont des actes législatifs contraignants. Ils doivent être mis en œuvre dans leur intégralité, dans toute l'Union européenne. Par exemple, lorsque le règlement de l'UE sur la suppression des frais d'itinérance à l'intérieur de l'Union a expiré en 2022, le Parlement et le Conseil ont adopté un nouveau règlement, à la fois pour améliorer la clarté du règlement précédent et pour garantir l'application d'une approche commune en matière de frais d'itinérance pour une nouvelle période de dix ans.

Définition des acteurs

Fabricants, exploitants, fournisseurs, distributeurs, autorités compétentes, etc.

Se réfère à une norme si nécessaire

De manière obligatoire
De manière indirecte : les normes offrent une présomption de conformité.
Cela permet de prouver qu'on respecte une directive européenne (ex.: sécurité machine, compatibilité électromagnétique…).
Normes harmonisées

Update Cybersécurité

Directive NIS2

Objectif

Cybersécurité des moyens de production des entreprises et des administrations de l'Union Européenne

Cyber Resilient Act

Objectif

Cybersécurité pour les produits matériels ou logiciels vendus dans l'Union Européenne (Grand Public, Administration, Entreprise)

L'Europe en première ligne **face aux cybermenaces**

La directive NIS2 conduit les entités à travailler sur les aspects de la chaine de cybersécurité dans sa globalité :

- Gouvernance
- La formation
- Analyse de risque & procédures
- Gestion des incidents
- Technologie
  - Gestion des utilisateurs et des droits d'accès
  - Gestion des configurations Et mise à jour des produits
  - Cryptographie
  - Suivi des actions

LACROIX

Avec la directive NIS2,

l'Union Européenne et la France **renforcent leur arsenal réglementaire et méthodologique**

NIS2 : de l'adoption **à l'application**

Dates & Statut en France

2021
Négociations européennes autour de la révision de NIS1

2022
27 décembre 2022
Publication de la directive NIS2 au Journal Officiel de l'UE

2023
Janvier 2023
Entrée en vigueur de la directive NIS2 au niveau européen

2024
17 octobre 2024
Échéance de transposition nationale pour les États membres

PROJET DE LOI FRANÇAISE EN COURS

2025
17 janvier 2025
Les États membres informent la Commission européenne des règles et mesures adoptées

17 avril 2025
Chaque État membre établit la liste des EE et EI

Votre entité est-elle assujettie à la directive NIS2 ?

FAITES LE TEST

Diagnostic cybersécurité **gratuit**

Acteurs concernés par NIS2

QUI EST CONCERNÉ ?

Les entreprises

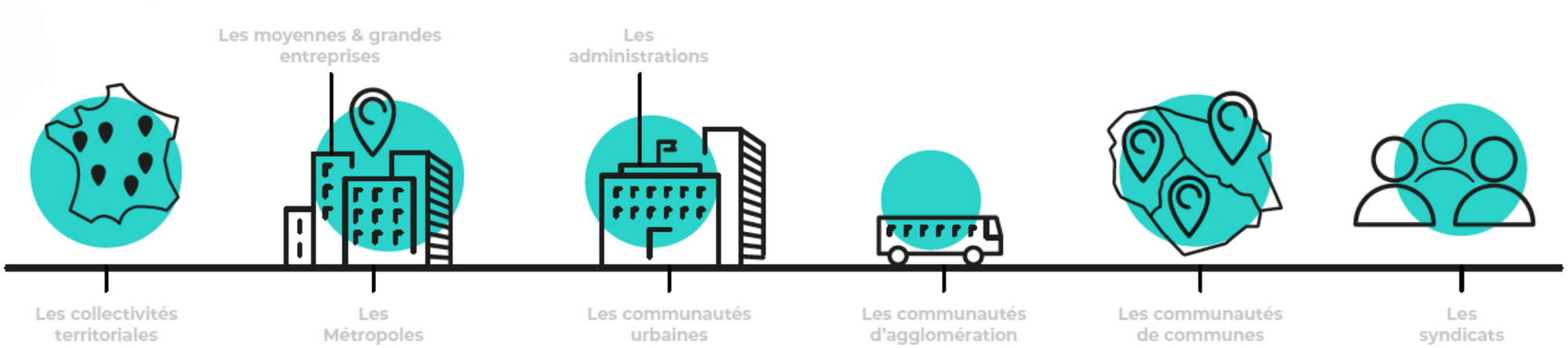
Entités Essentielles (EE)
- > 250 salariés
- CA > 50 M€ ou bilan > 43 M€
- Secteurs hautement critiques : eau, énergie, santé, numérique, transport, etc.

Entités Importantes (EI)
- > 50 salariés
- CA > 10 M€ ou bilan > 10 M€
- Autres secteurs critiques : industrie, agroalimentaire, logiciels, recherche, etc.

Les collectivités territoriales

Les collectivités territoriales seront concernées. Leur classement en tant qu'**Entités Essentielles (EE)** ou **Entités Importantes (EI)** sera définit lors de la finalisation de la loi française

👉 Responsabilité maintenue même en cas de délégation à un prestataire



Acteurs concernés par NIS2

LES AGENCES DE RÉFÉRENCES

ENISA *(Europe)* : définit et harmonise les bonnes pratiques, promeut un niveau commun de cybersécurité

ANSSI *(France)* : pilote la transposition, accompagne les acteurs, supervise la conformité.

Votre entité est-elle assujettie à la directive NIS2 ?

Diagnostic cybersécurité **gratuit**

LES SANCTIONS EN CAS DE NON-APPLICATION DE NIS2

Pour les entreprises privées

- **Jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel** mondial pour non-respect des obligations.
- Possibilité d'audits, injonctions et **suspension des dirigeants**.

Pour les Entités publiques

- **Non encore légiféré.** Sanctions en cours de définition.

Les secteurs concernés par NIS2

SECTEURS HAUTEMENT CRITIQUES

- Administrations publiques
- **Eau potable**
- **Eaux usées**
- **Énergies**
- Espace
- Gestion des services Technologies de l'Information et de la Communication (interentreprises)
- Infrastructures des marchés financiers
- Infrastructures numériques
- Santé
- Secteur bancaire
- Transports

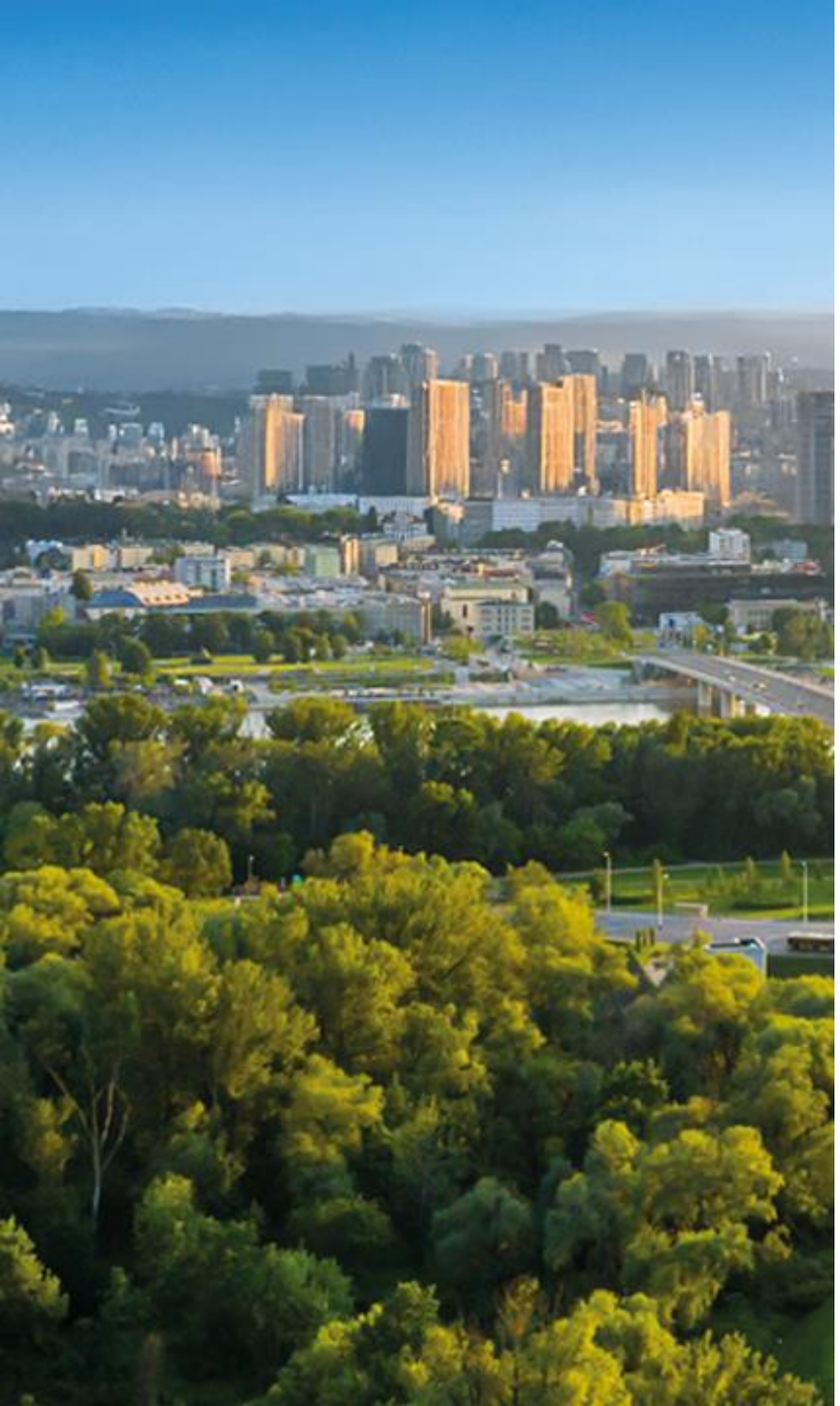
AUTRES SECTEURS CRITIQUES

- Fabrication, production et distribution de produits chimiques
- Fournisseurs numériques
- Gestion des déchets
- Industrie manufacturière
- Production, transformation et distribution de denrées alimentaires
- Recherche
- Services postaux et d'expédition

Les mesures à mettre en œuvre

DÉFINIES DANS L'ARTICLE 21

- Les politiques relatives à **l'analyse des risques** et à la sécurité des systèmes d'information ;
- La **gestion des incidents** ;
- La **continuité des activités**, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;
- La **sécurité de la chaîne d'approvisionnement**, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;
- La sécurité de l'acquisition, du développement et de la **maintenance** des réseaux et des systèmes d'information, y compris le traitement et la **divulgation des vulnérabilités** ;
- Des politiques et des procédures pour évaluer l'efficacité des mesures de **gestion des risques** en matière de **cybersécurité** ;
- l'utilisation de la **cryptographie** et, le cas échéant, du **chiffrement** ;
- La sécurité des **ressources humaines**, des politiques de **contrôle d'accès** et la gestion des actifs ;
- L'utilisation de **solutions d'authentification** à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.



AGENDA

01 Cybersécurité dans l’eau, mythe ou réalité ?

02 Cybersécurité: Directive NIS2

03 Cybersécurité: Règlement CRA

04 Conclusion

Cyber Resilience Act

DATES & STATUT EN EUROPE

L'adoption du texte relatif au CRA date de 2024.
Pour les fabricants, son application se fera selon les étapes suivantes :

CRA

Règlement (UE) 2024/2847, est un règlement de l'Union européenne visant à renforcer la cybersécurité des produits comportant des éléments numériques commercialisés dans l'Union européenne. Il s'applique donc dans tous les pays de façon identique.

Acteurs impactés

Tous les fabricants, importateurs, distributeurs mettant des produits sur le marché européen doivent conforme avec le CRA

Produits impactés

Logiciels, matériel avec logiciel embarqué, services hybrides (Service cloud nécessaire au bon fonctionnement d'un produit, application avec un composant local (agent, SDK))*

Obligations

Conception sécurisée | Pas de failles connues à la livraison | Protections des données | Mise à jour obligatoires pendant 5 ans après la fin de commercialisation
Gestion des vulnérabilités | Configuration sécurisée par défaut | SBOM *(Software Bill of Material)*

Sanctions

Interdiction de ventes
Rappel des produits vendus
Retrait des produits du marché

Jusqu'à 15M€ ou 2% du CA

* Hors pur SaaS, projet opensource, médical, automobile, aviation, équipements militaires

Conception sécurisée

- Protéger contre les accès non autorisés (authentification, contrôle d'accès)
- Garantir la confidentialité des données
- Garantir l'intégrité des données (pas de modification non autorisée)
- Minimiser la surface d'attaque (désactiver ce qui n'est pas nécessaire)
- Limiter les dégâts en cas d'incident (moindre privilège)

Protection des données

Protection des données personnelles

Suppression par l'utilisateur

Données collectées limitées au strict nécessaire

Pas de failles connues à la livraison

Un produit mise sur le marché doit être exempte de vulnérabilités connues et exploitables

Configuration sécurisée par défaut

Mise à jour automatique activée ou incitation forte)

Pas de mot de passe par défaut faible ou identique

Fonctionnalités sensibles désactivées par défaut

Gestion des vulnérabilités

- Signalement
- Priorisation
- Correctifs
- Communication

SBOM
(Software Bill of Material)

Software bill of materials – la liste des composants logiciels dans les produits – permet d'identifier les vulnérabilités cyber (CVE (Common Vulnerabilites Enclosures), internes etc.)

Mise à jour obligatoires

Obligation de fournir des mises à jour pendant 5 ans après la fin de commercialisation

Acteurs impactés

Fabricant

Conception du produit

Assurer la conformité complète, générer la SBOM, maintenir les mises à jour

Importateur

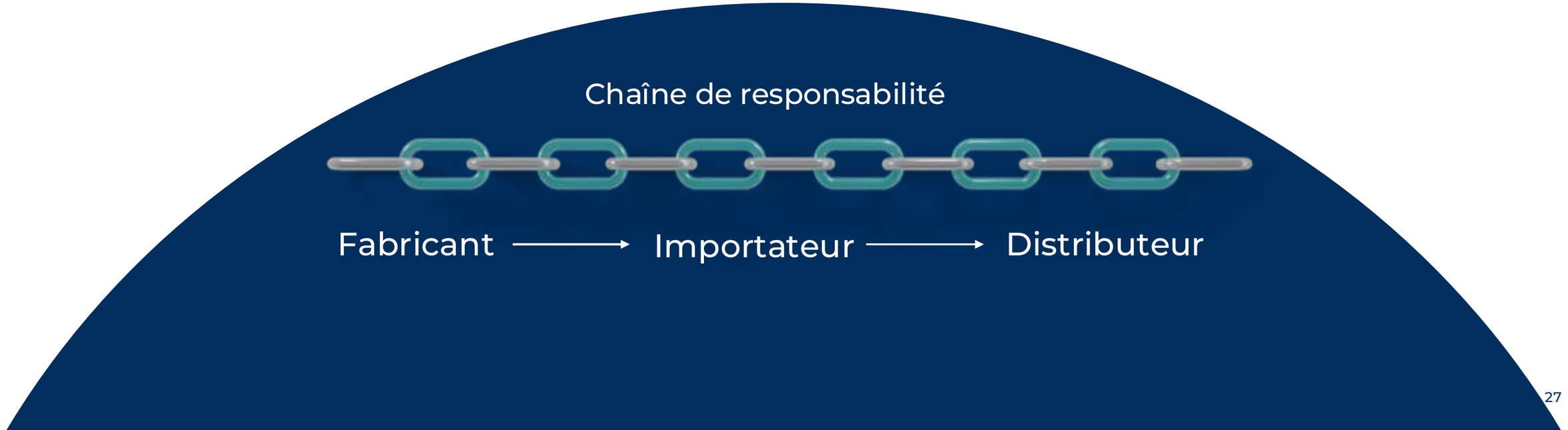
Importation du produit non EU sur le marché européen

Vérification que la fabrication est conforme au CRA, pas d'importations de produits non conformes, vérification marquage

Distributeur

Distribution du produit non EU sur le marché européen

Vérification que la fabrication est conforme au CRA, vérification marquage, retraits de produits non conformes



Mise à jour

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(j) be designed, developed and produced to limit attack surfaces, including external interfaces;

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

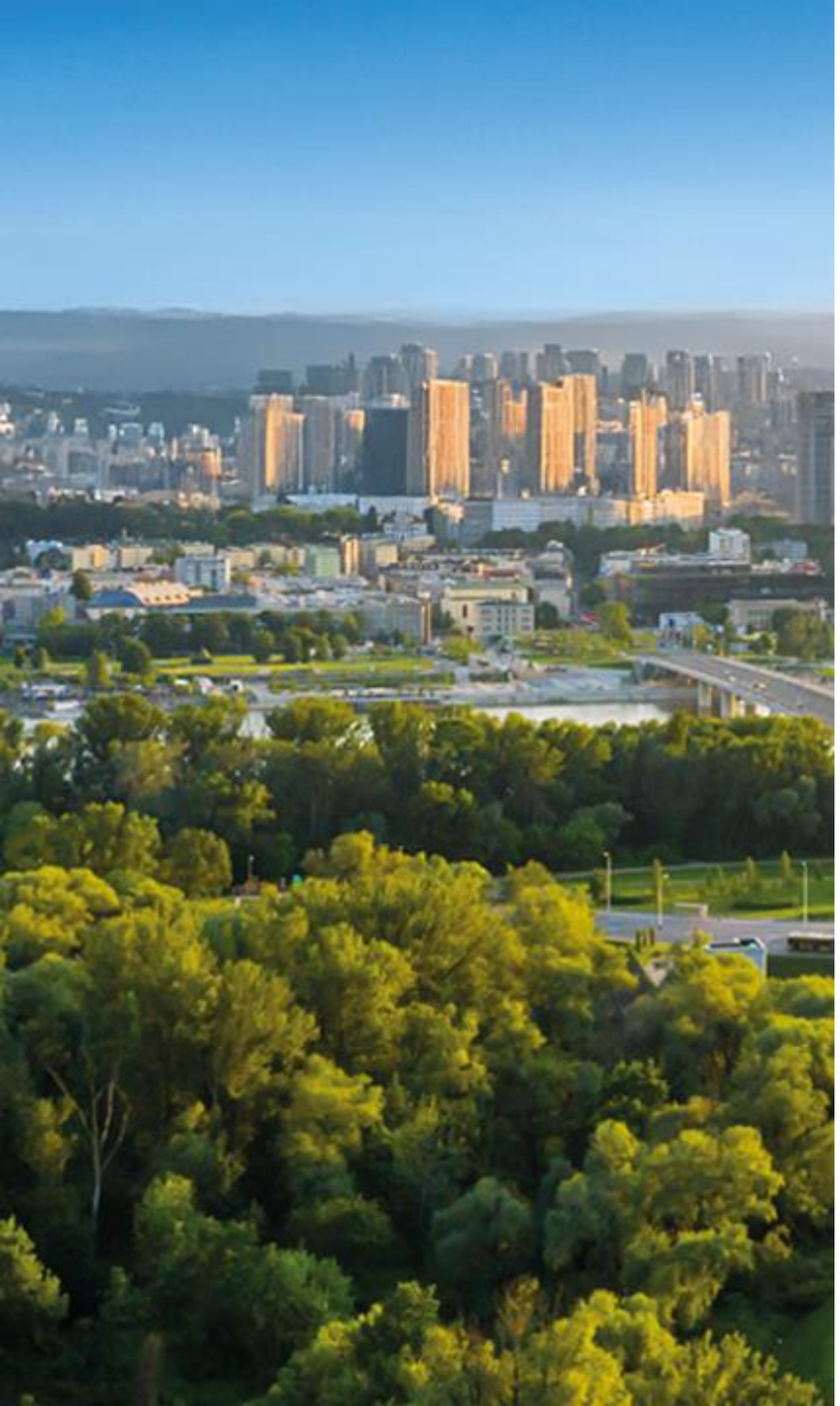
(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.



AGENDA

01 Cybersécurité dans l’eau, mythe ou réalité ?

02 Cybersécurité: Directive NIS2

03 Cybersécurité: Règlement CRA

04 Conclusion

LES DÉFIS

POUR EXPLOITER UN RÉSEAU DE TÉLÉGESTION EN 2026

TOUT IP

Migration des réseaux

Remise à plat des architectures historiques de télégestion

Nouvelles possibilités de déploiement et d'hébergement des applications métiers

Réflexions à mener entre les équipes métiers et les équipes IT

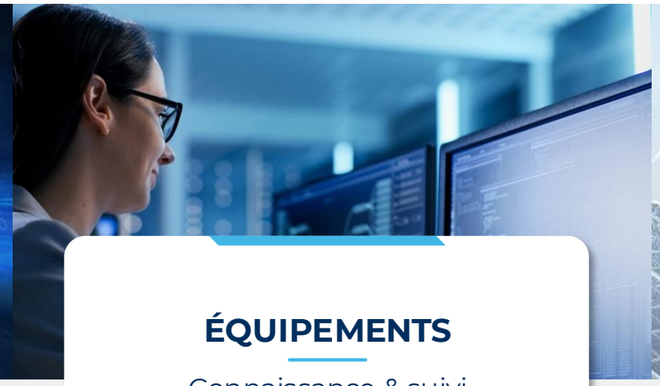
CYBERSÉCURITÉ

Mise en place & administration

Nouvelles compétences à acquérir pour les équipes métiers

Nouveaux processus à mettre en place dans le déploiement et l'administration d'un parc

Réflexions à mener entre les équipes métiers et les équipes IT



ÉQUIPEMENTS

Connaissance & suivi

Difficulté de bien suivre et tracer l'état d'un parc d'équipements

MISE À JOUR

Parc d'équipements

Processus indispensable pour déployer les nouvelles versions logicielles et appliquer les derniers patchs de sécurité

Nécessité de se déplacer ou de se connecter à distance sur chacun des sites pour mettre à jour une nouvelle version logicielle (firmware)

Les opérateurs

La réglementation européenne conduit les entités à travailler sur les aspects de la cybersécurité :

- Les exploitants
- Régie
- Métropoles, (etc)

NIS2 Network & Information Systems Directive

- ISO 27001
- IEC 62443
- Ou autres méthodes équivalentes

Les fabricants

Pour les fabricants :

Fabricants

- NIS2 — Network & Information Systems Directive
- CRA — Cyber Resilience Act

- ISO 27001
- IEC 62443
- Ou autres méthodes équivalentes

LX CONNECT, la plateforme de centralisation des équipements LACROIX SOFREL

LX CONNECT
Nouvelle brique clé de la gestion cybersécurisée des réseaux d'eau, de chauffage et d'énergie

La cybersécurité automatisée des équipements

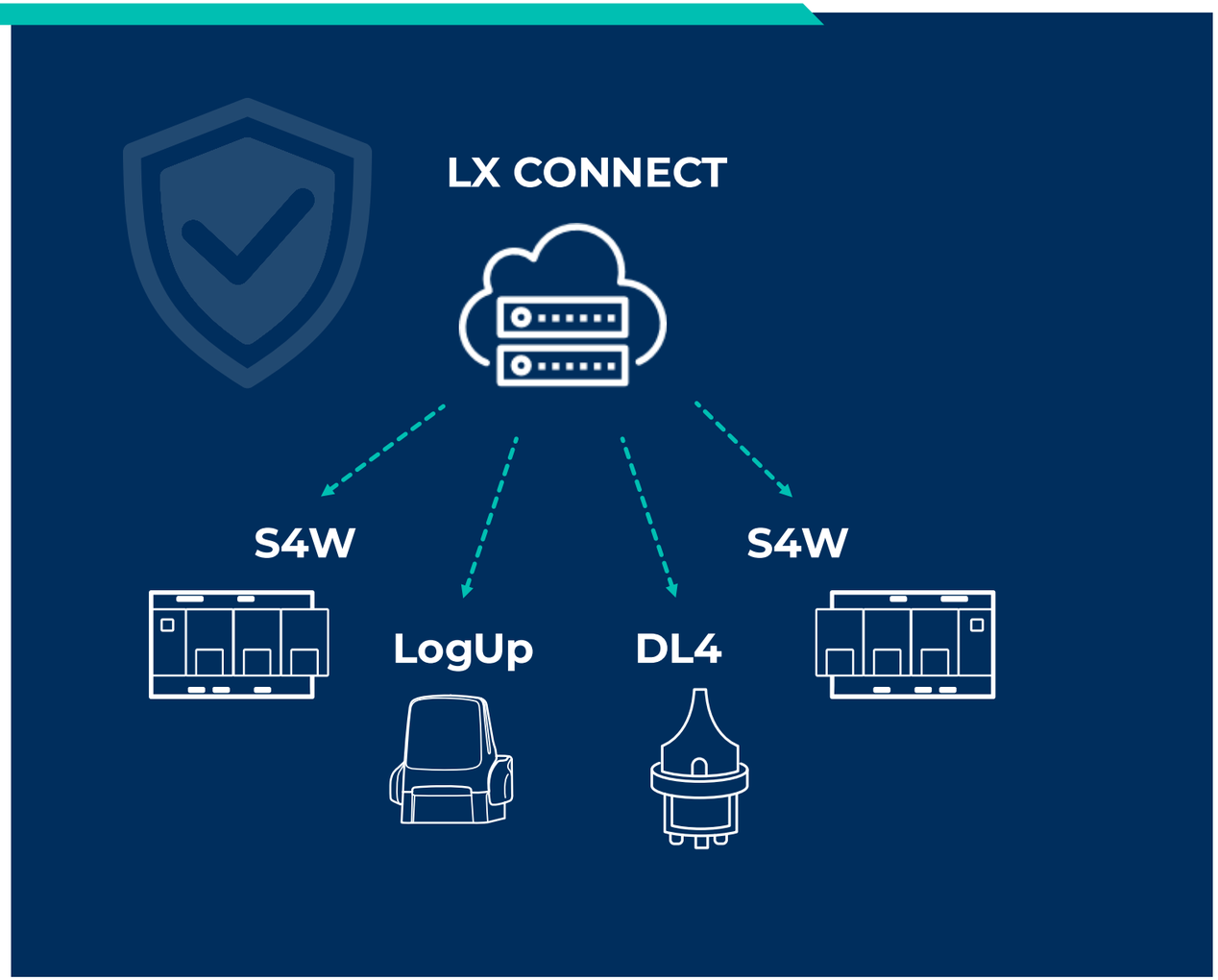
La gestion à distance d'un parc d'équipements multisites

La traçabilité des opérations menées sur les utilisateurs

La centralisation des données métiers et systèmes des équipements

L'interopérabilité avec les applications tierces (SCADA) pour partage des données et pilotage à distance des sites

Une solution conforme aux enjeux futurs en matière de cybersécurité



- Gestion des utilisateurs
- Mise à jour à distance des équipements
- Chiffrements des communications
- Gestion et suivi des vulnérabilités
- Suivi des actions utilisateurs
- Renouvellement automatique des certificats

Merci de votre attention

To find out more, explore our websites and stay connected with us!

LACROIX Activity Electronics Activity Environment

Alexander Foote
Co-pilote du groupe de travail cybersécurité ASTEE

www.akandu.fr

Le référentiel cybersécurité ASTEE

Qu’est-ce qui a changé ?

- Evolution des menaces
  - De nouvelles cibles (PME, ETI, Collectivités)
  - De nouvelles technologies industrielles TCP/IP et intégrations IT
  - Le rôle de l’IA
- NIS2
  - Plusieurs dizaines de milliers d’entités concernées.
  - 18 secteurs d’activités concernés dont l’alimentation en eau potable, l’assainissement et les déchets
  - Obligation de mettre en œuvre la réglementation relative à la cybersécurité.
  - Collectivités > 30k habitants ?

Pas que de la théorie

Le SMDEA, victime d'une cyberattaque

Accueil › Actualités › Le SMDEA, victime d'une cyberattaque

SMDEA 09
NOS COMPÉTENCES AU SERVICE DE L'EAU

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFECTURE

LES FAITS

Le dimanche 14 mai 2023, le SMDEA a été victime d'une cyberattaque sur son infrastructure

- **SMDEA (mai 2023) et Angers Loire Métropole (janvier 2021) :**
  - SMDEA : vol de données des abonnés ensuite encryptées, puis demande de rançon pour obtenir la clé de décryptage, avec la menace de voir ces données sensibles exposées au grand jour sur le web ;
  - Impacts sur les données personnelles des usagers ;
  - Risques d'usurpation d'identité les ciblant ultérieurement ;
  - Impact sur la facturation des clients ;
  - Perturbations très sérieuses sur les relations clients ; …

Le Référentiel Cybersécurité Astee

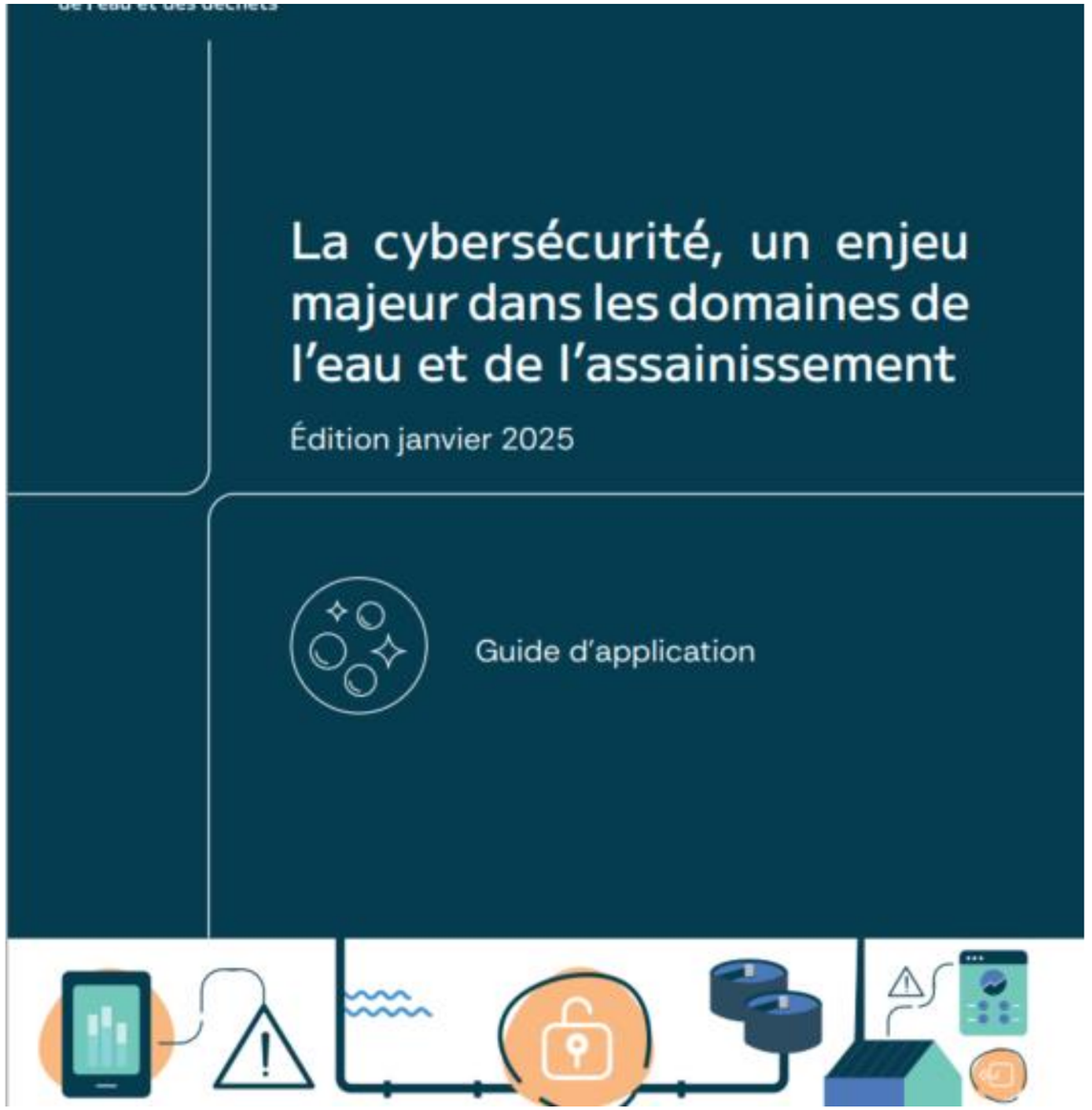
- **Le groupe de travail**
  - Des collectivités, des exploitants et des spécialistes de la cybersécurité
- **Objectifs**
  - Un référentiel adapté aux petites et moyennes collectivités dans les domaines de l'eau potable et de l'assainissement
    - Guide de bonnes pratiques accessible à tous
    - Conseils détaillés par thème d'action à mener
    - Critères hiérarchisés pour évaluer la maturité des dispositifs et équipements industriels vis-à-vis du risque cyber
  - Des documents types (cahier des charges audit et article type DSP / Prestation de service)
- **Mise à disposition janvier 2025**

astee

Guide Astee et NIS2 : Complémentarités

	Guide Astee	NIS2
Taille organisation	Petites et moyennes collectivités	> 30k habitants ?
Conformité	Niveaux 0-4	Oui/Non
Objectif	Ciblé industrie eau	Général
Disponible	Maintenant	Printemps/été 2026? Document ReCyf disponible.

Présentation du guide



Le Référentiel

- 0 - Prérequis
- 1 - Responsabilité des acteurs
- 2 - Connaissance du système d'informatique industrielle
- 3 - Sécurité de l'architecture informatique industrielle
- 4 - Sécurité des accès physiques
- 5 - Sécurité des accès logiques
- 6 - Maitrise et configuration des équipements
- 7 - Maintenance et gestion des changements
- 8 - Détection et traitement des incidents
- 9 - Sauvegardes et continuité du service
- 10 - Audit, contrôle, suivi des indicateurs
- A - Eléments contractuels
- B - Sensibiliser et former le personnel de la collectivité

astee

0. Prérequis

Pour mettre en œuvre une politique de cybersécurité sur ses installations, il conviendra d'identifier les systèmes d'information et pour chacun d'eux, leur niveau de criticité et de sensibilité au regard du métier. Pour cela une analyse de risque constitue le prérequis indispensable à la poursuite d'une démarche de sécurisation.

			STRUCTURE			
			PETITE		INTERMÉDIAIRE	
Priorité 1 -3	Questions à se poser	Évaluation 0-4	Objectif	Conseils	Objectif	Conseils à appliquer en supplément des petites structures
1	Quel est le périmètre de vos services d'eau et d'assainissement à inclure prioritairement dans la démarche cybersécurité ?	**0-** Le périmètre n'est pas défini. **1-** Le périmètre n'est pas défini mais la démarche est en cours. **2-** Le périmètre inclut a minima un secteur des services industriels. **3-** Le périmètre intègre complètement un service industriel. **4-** Les services sont tous inclus dans le périmètre.	4	À définir pour tout ou partie des entités de gestion et des services (eau, assainissement, distribution, production, collecte, traitement...).	4	Idem petite structure.
1	Avez-vous mené une analyse afin d'évaluer la criticité et la sensibilité de vos équipements et systèmes d'informatique industrielle ?	**0-** L'analyse de risques n'a pas été réalisée. **1-** Une analyse informelle des risques liés aux principaux composants du système industriel a été réalisée. **2-** L'analyse de risque des principaux composants a été réalisée. **3-** L'analyse de risque de tous les composants a été réalisée. **4-** L'analyse de risque a été réalisée et est revue régulièrement.	2	Les dysfonctionnements de l'informatique industrielle sont à prendre en compte en réalisant une analyse des risques industriels et de leurs impacts sur la continuité de service et sur les aspects sanitaires, environnementaux, juridiques et économiques.	4	Idem petite structure.

Les bonnes pratiques

- 10 règles de la cybersécurité IT sur site industriel
- Etablir un PRA et PCA
- Exemple d’article contractuel
- Cartographier son IT
- Méthodologie d’évaluation de sensibilité d’un site
- Rédiger un CdC d’audit de maturité cyber

astee

Comment utiliser le guide

- Ce n’est pas uniquement pour le technicien !
- Un travail de plusieurs années.
- Ca commence par un état des lieux.
- Priorisation des projets, avec un budget associé.
- Commencer tôt car NIS2 arrive…

Prochaines Etapes

- Téléchargez le guide sur **www.astee.org** et diffusez-le aux professionnels de vos réseaux !
- Journées prises-en-main portées par les sections territoriales Astee.
- Formation Watura Astee+NIS2

https://www.astee.org/publications/guide-dapplication-la-cybersecurite-un-enjeu-majeur-dans-les-domaines-de-leau-et-de-lassainissement/

AKANDU

Alex Foote
alexander.foote@akandu.fr

Les Etanchéités Dynamiques

Garnnitures Mécaniques et Tresses

Laurent Sant / Laurent Prunier Duparge

Mai 2026 | Paris

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Chesterton hier aujourd’hui et demain

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Notre histoire

142 années d'engagement pour rendre nos clients plus productifs, rentables et respectueux de l'environnement.

Notre vision

Etre au plus haut a l’esprit de nos clients par l’innovation et l’excellence

“Nous croyons qu'un esprit curieux et imaginatif favorise l'innovation. Nous sommes curieux et enthousiastes à l'idée de travailler avec les clients pour résoudre leurs problèmes, et les soutenir par un succès démontré à travers l’industrie.”

Andrew Chesterton, President and CEO

Siège social

Groveland, Massachusetts I USA

Création:

1884 à Boston, Massachusetts

Effectifs:

Plus de 1,300

Couverture ventes:

120 Pays

Chiffre d’affaire:

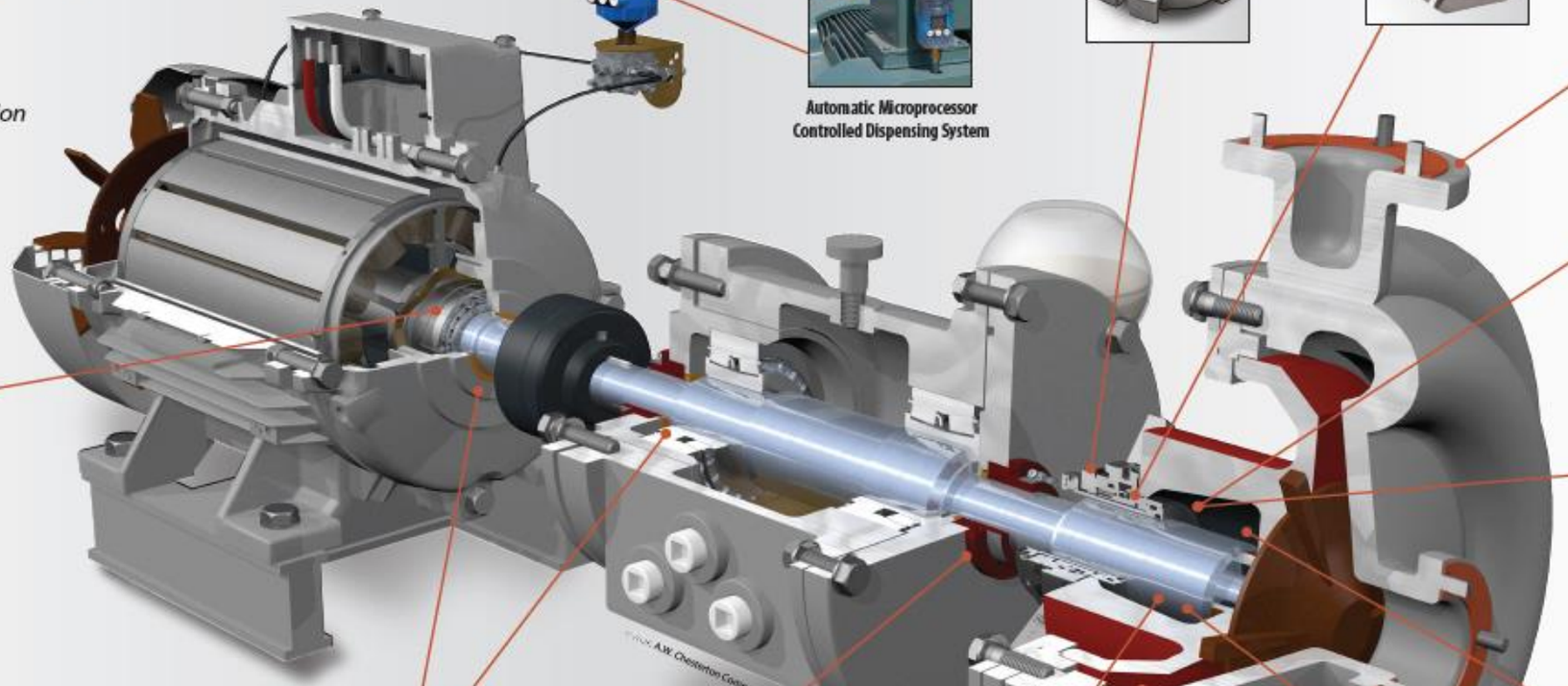
300 Million $

L'innovation est la base de notre succès

Notre succès est dans le développement de solutions innovantes qui provient d'un processus interne solide qui identifie clairement les défis la où nos clients ont besoin de solutions inventives.

Chesterton® Solutions for Rotating Equipment

Whether advanced shaft sealing, gearbox protection, system lubrication, or protective coatings, Chesterton provides the total solution for improved pump reliability.



Advance Lubrication Technology

Automatic Microprocessor Controlled Dispensing System

Split Seals

Cartridge Seals

Gaskets – Sheet and Cut

Pump Packings

SpiralTrac® P Device

Restriction Bushings

Engineered Stuffing Box Seals

Bearing Protection Lip Seal

Split Polymer Labyrinth Seal

Environmental Controls

Protective Coatings for Metals

ARC INDUSTRIAL COATINGS

Other ARC Industrial Coatings

Machinable Composite

For Concrete & Metals

Other Maintenance and Repair Products

Electric Motor Cleaner

Anti-seizes

Thread Sealants

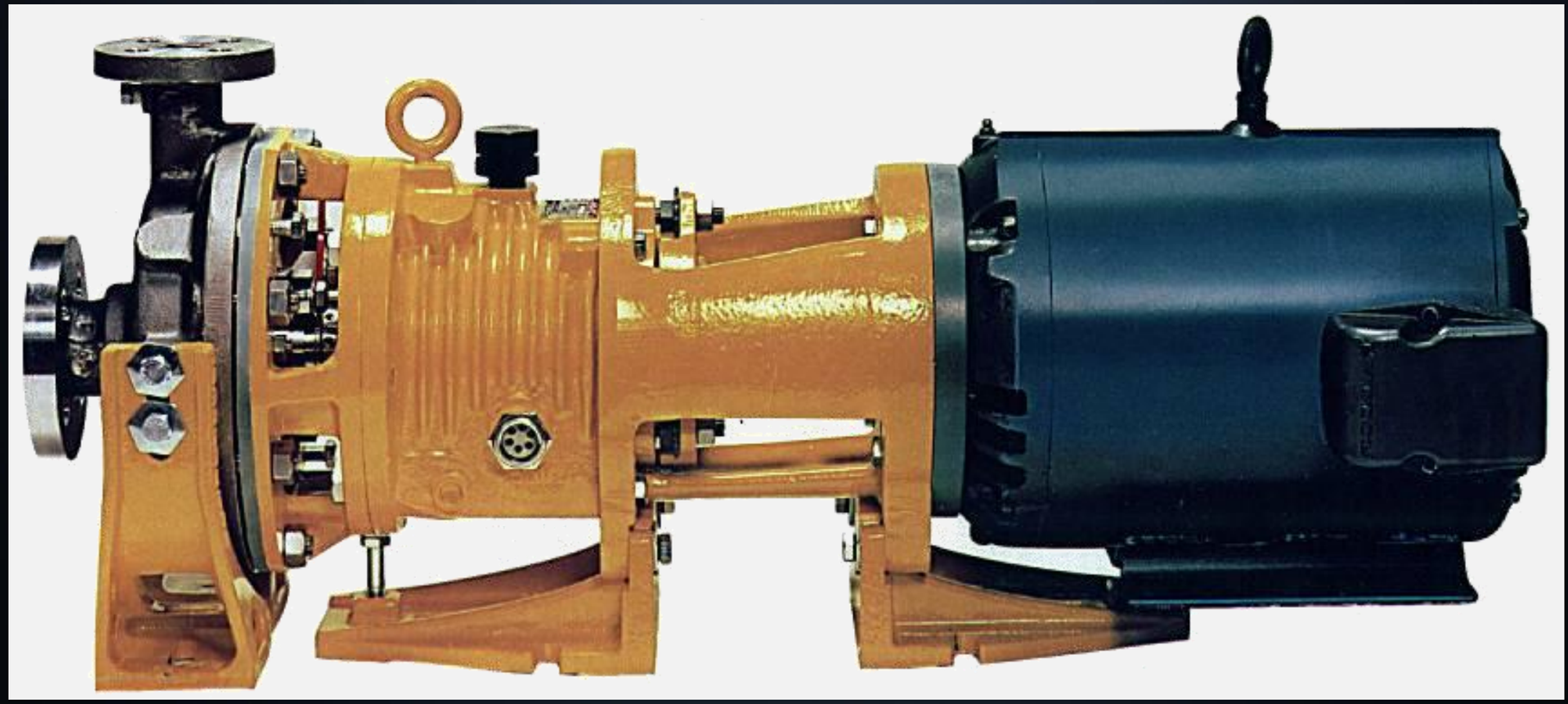
Moldable Gasketing

Introduction aux étanchéités dynamiques

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

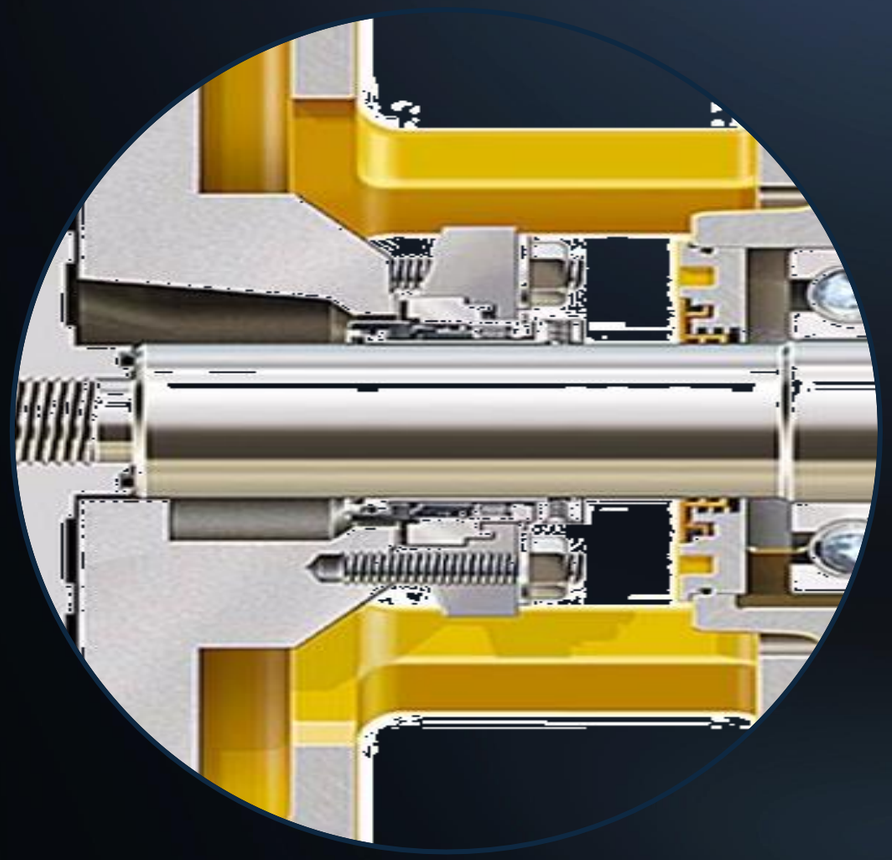
La Pompe Centrifuge

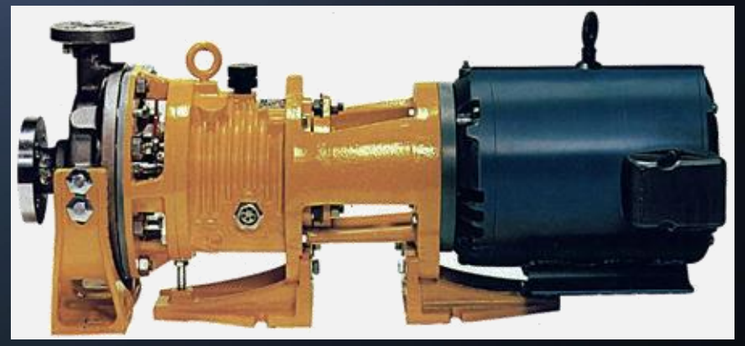


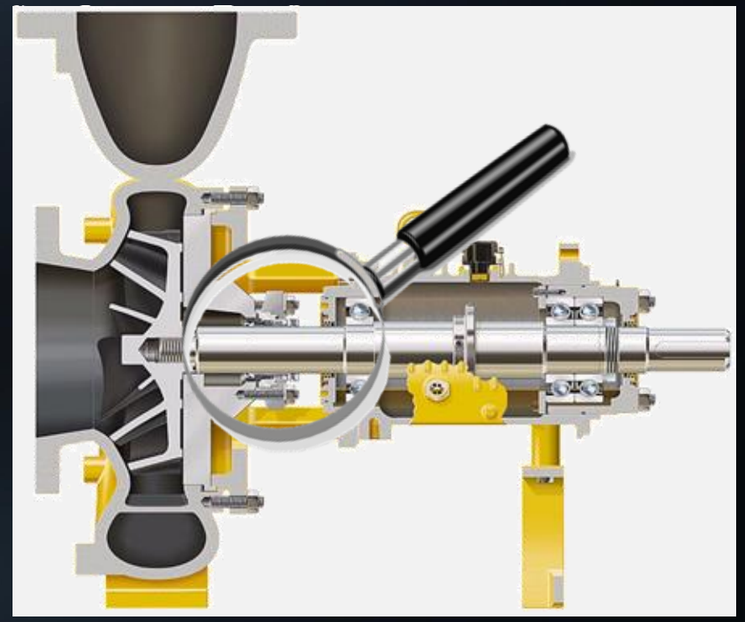
SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Dispositif d’étanchéité de sortie d’arbre





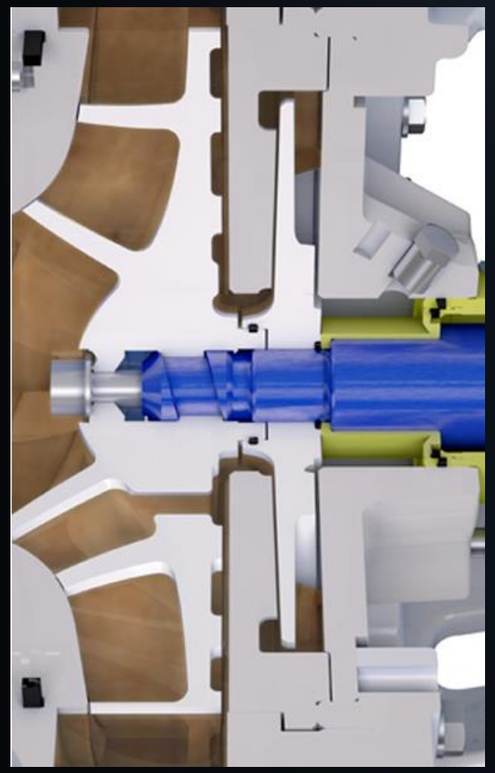


SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

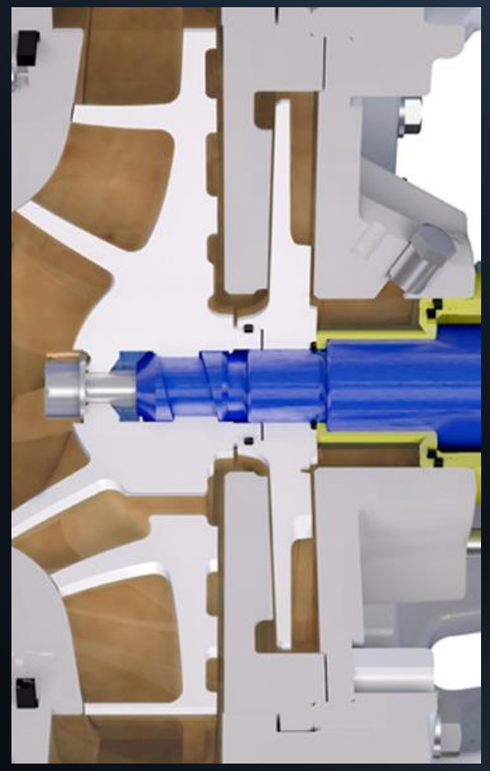
CHESTERTON
Global Solutions, Local Service.

Différents types d'étanchéités sur les pompes centrifuges

Pompe avec étanchéité hydrodynamique

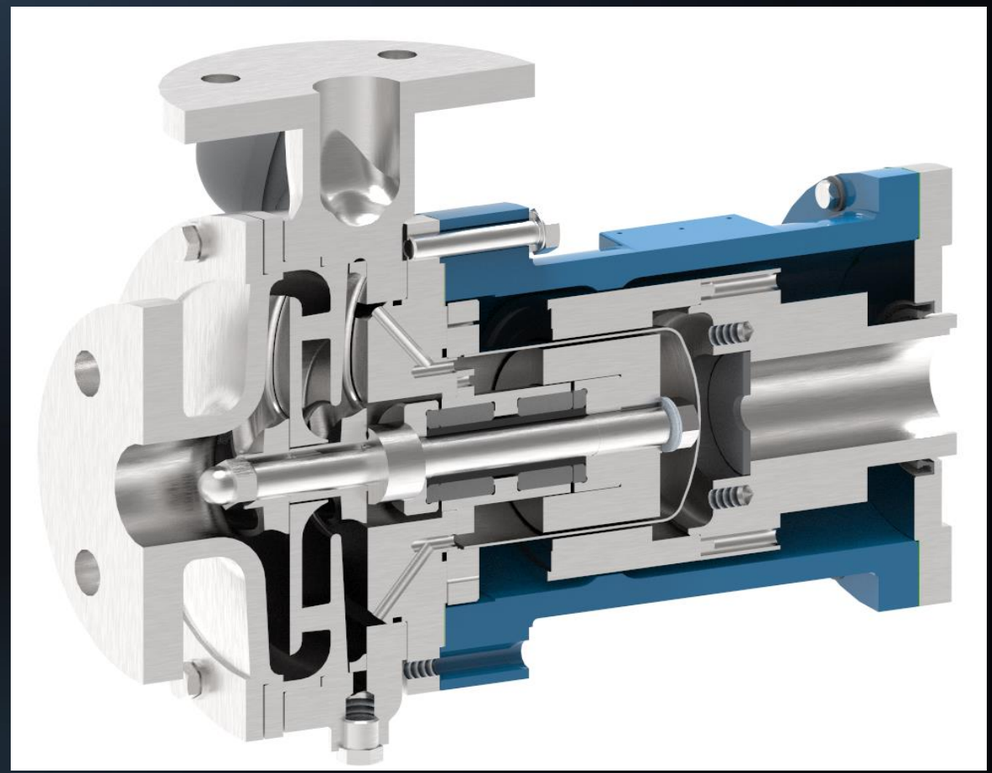


Pompe en fonctionnement



Pompe à l’arrêt

Pompe avec entraînement magnétique

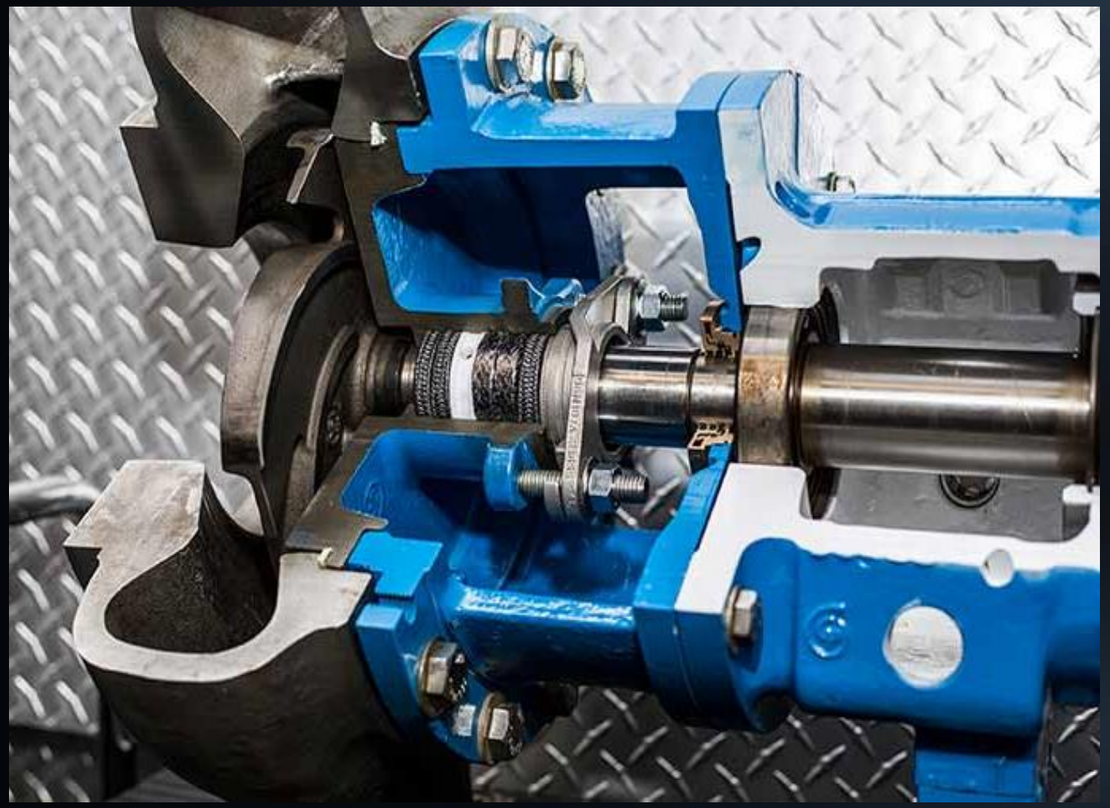


SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

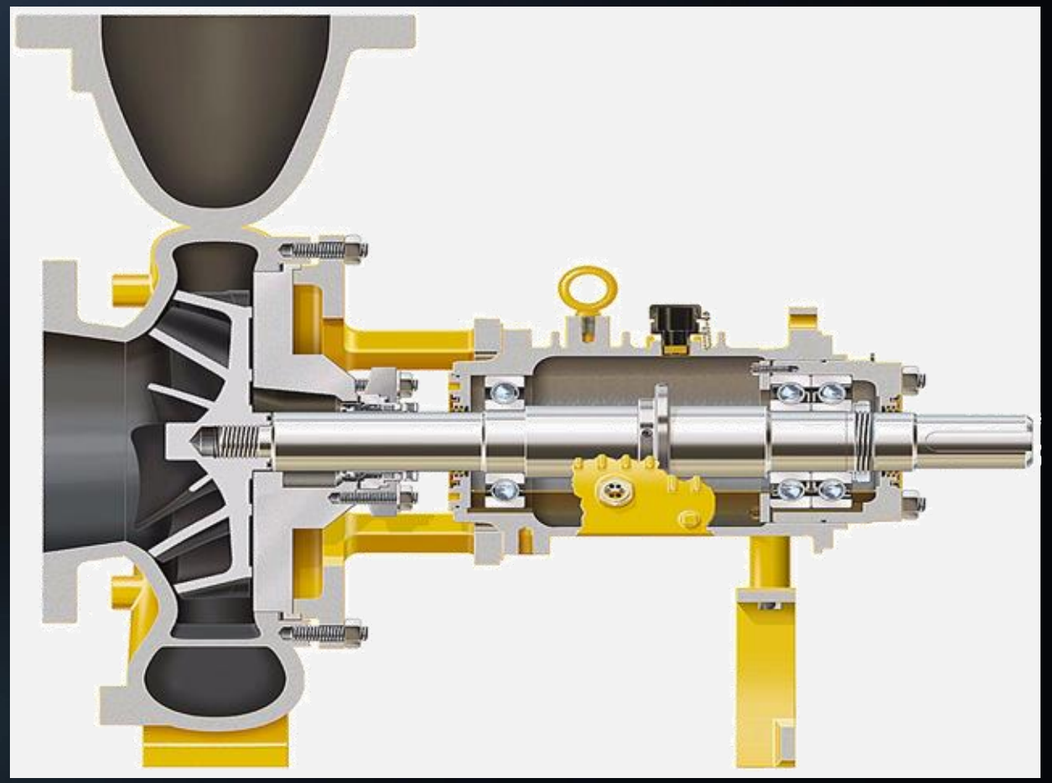
CHESTERTON
Global Solutions, Local Service.

Différents types d'étanchéités sur les pompes centrifuges

Pompe avec étanchéité par tresses



Pompe avec étanchéité par garniture mécanique



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

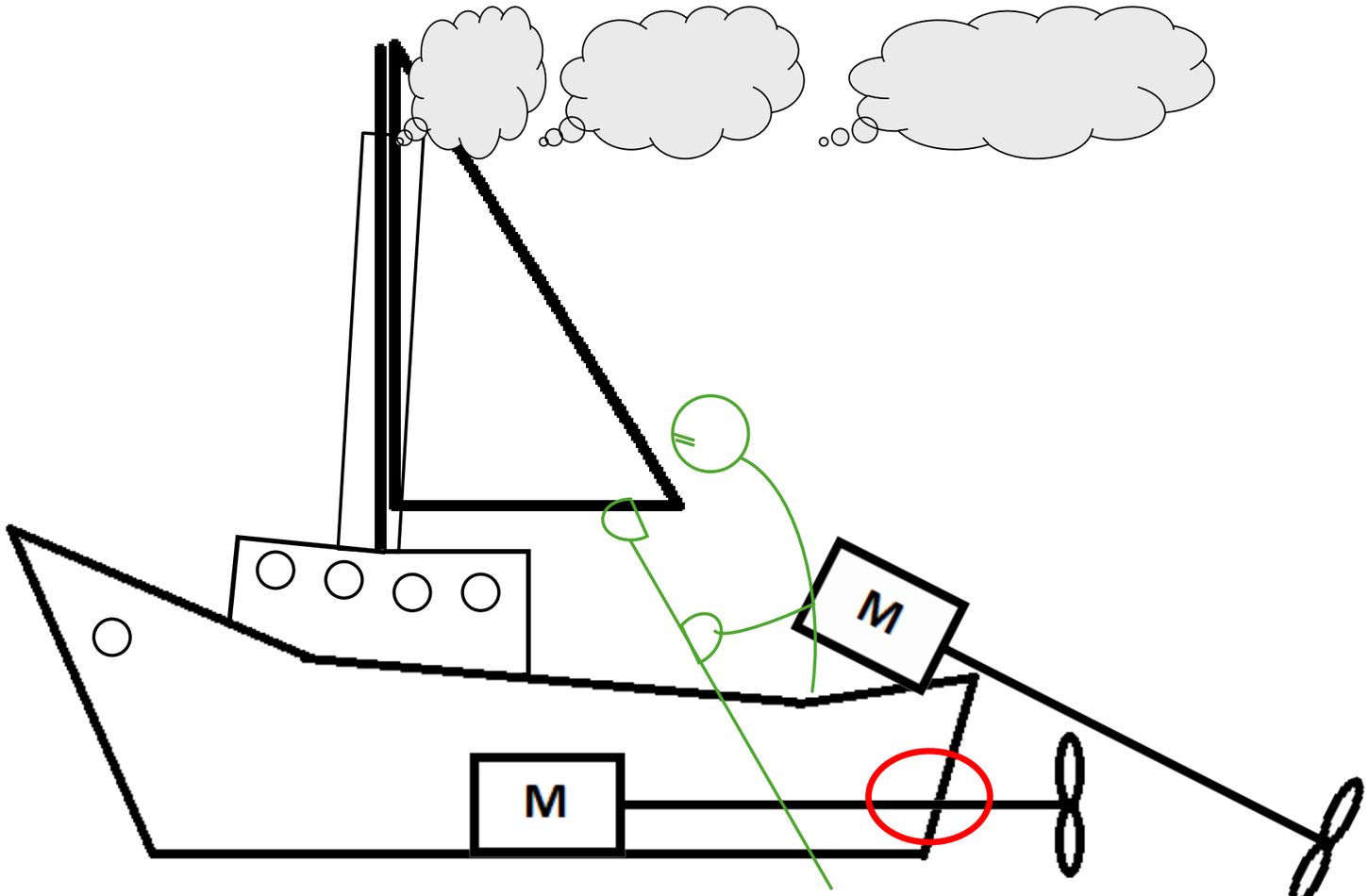
CHESTERTON
Global Solutions, Local Service.

Fonctionnement des tresses et Garnitures mécaniques

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

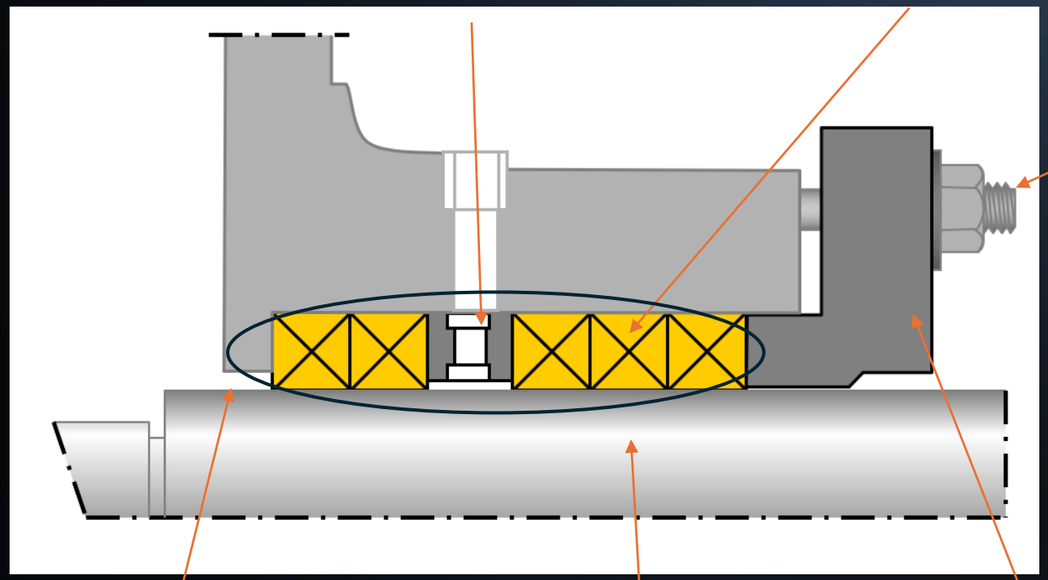
Bateau à propulsion



Presse étoupe

Bague lanterne

Tresses



Goujons
Écrous du Fouloir

Presse étoupe

Arbre de pompe

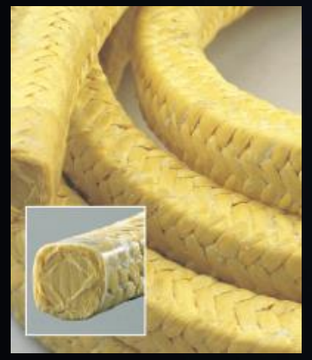
Fouloir

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Les principaux matériaux...

Fibre de Graphite ou de carbone
Pour les températures élevées. Dissipation calorique est importante. (Exemple d'application : eaux surchauffées)



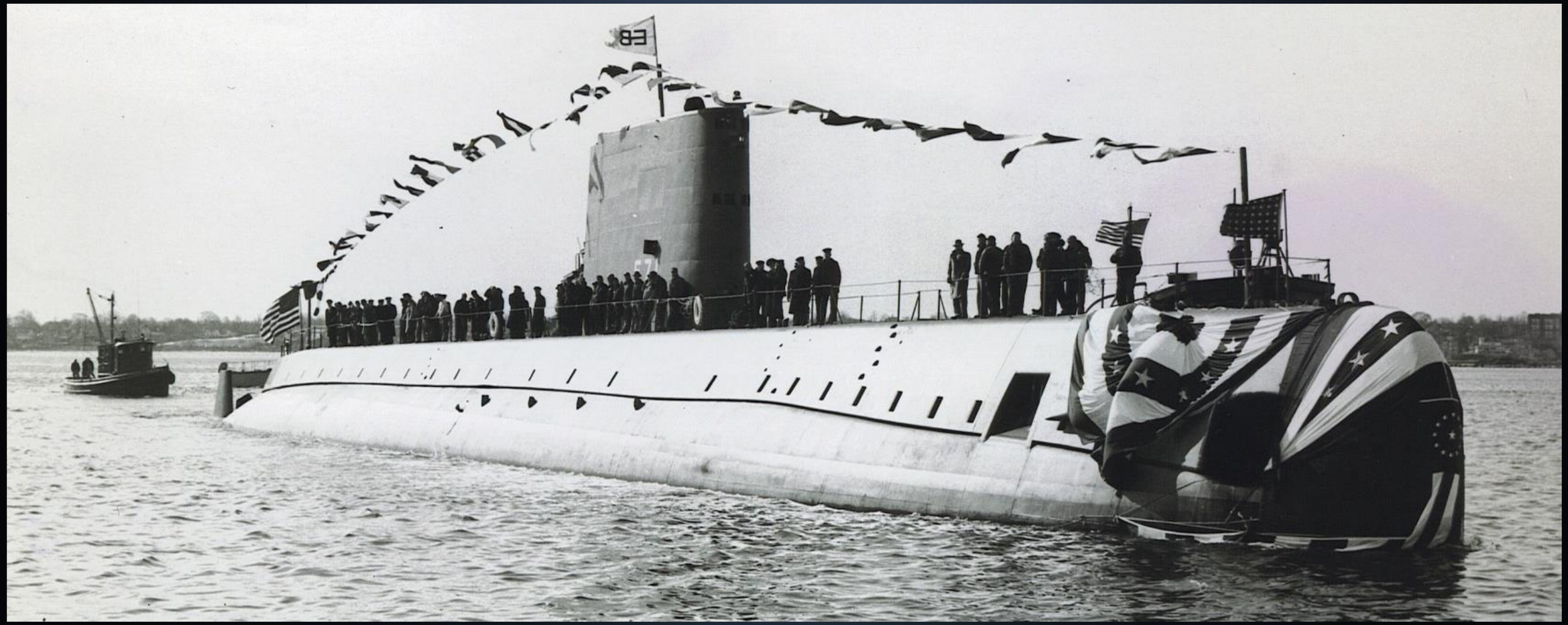
Fibre d'aramide
Pour les applications ou le produit véhiculé est abrasif. Bonne mémoire élastique dans le temps. Elle emmagasine néanmoins la chaleur et a tendance à user rapidement son support si celui-ci est trop tendre. (Exemple d'application : Eaux chargées).

Fibre de PTFE
Produits chimiques agressifs ou l'eau potable. Le PTFE améliore le coefficient de glissement de la tresse. Sa résistance à l'extrusion est limitée (fluage) notamment sur les anneaux de tresses localisés aux extrémités du presse étoupe. Les serrages excessifs ne sont donc pas admis. (Exemple d'application : Eaux potables).

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

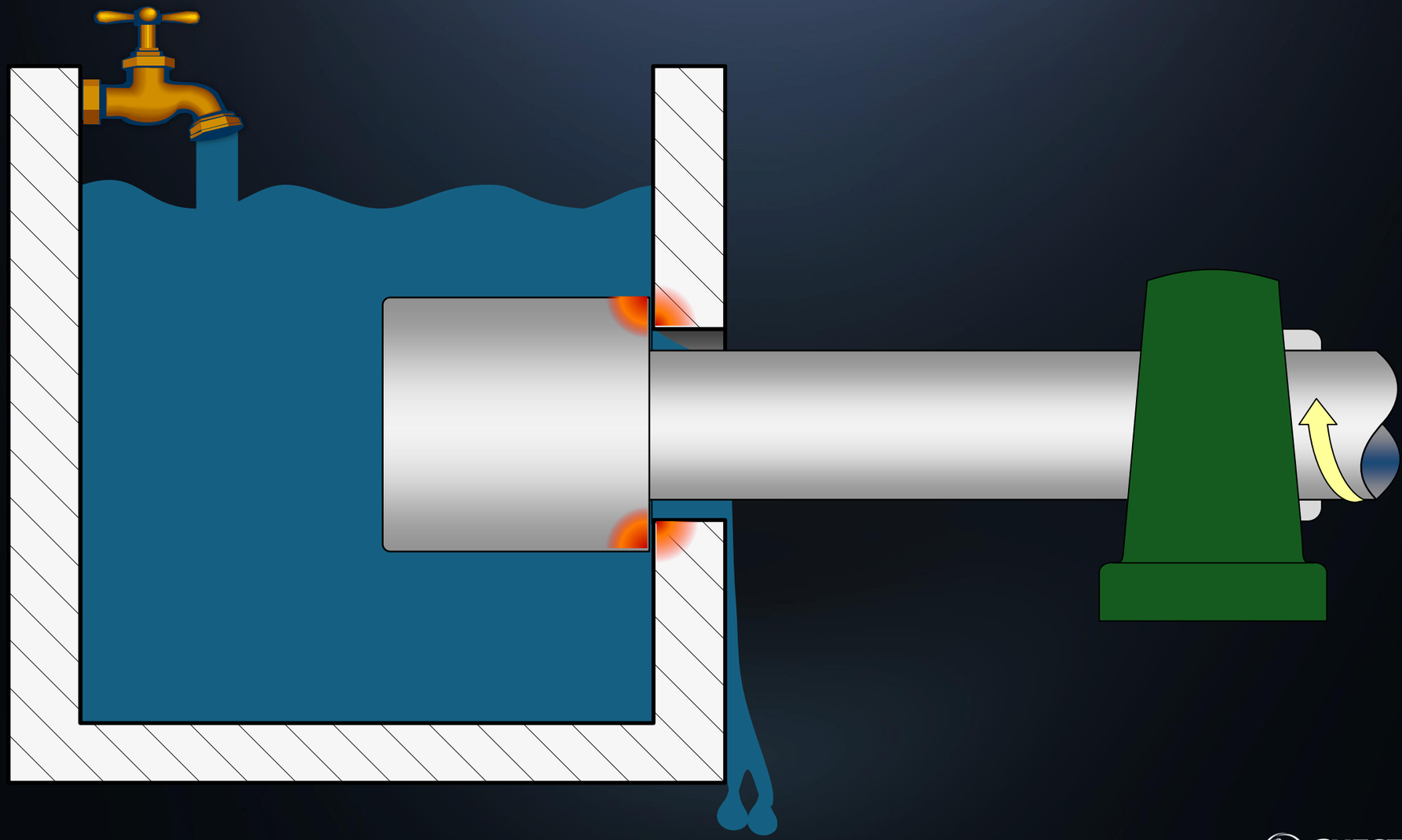
La Garniture Mécanique
De la tresse à la haute technologie…



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

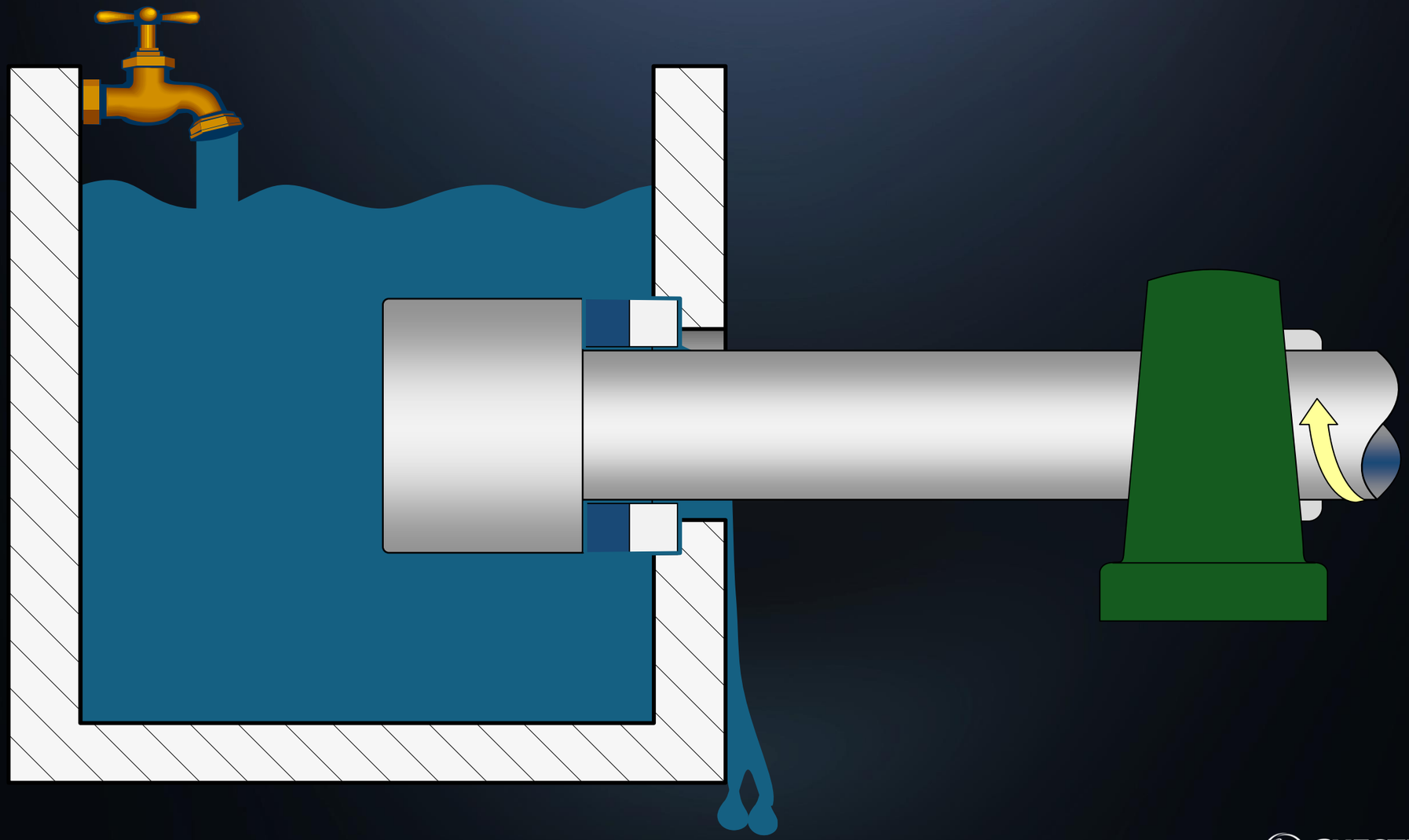
Etanchéite de base



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

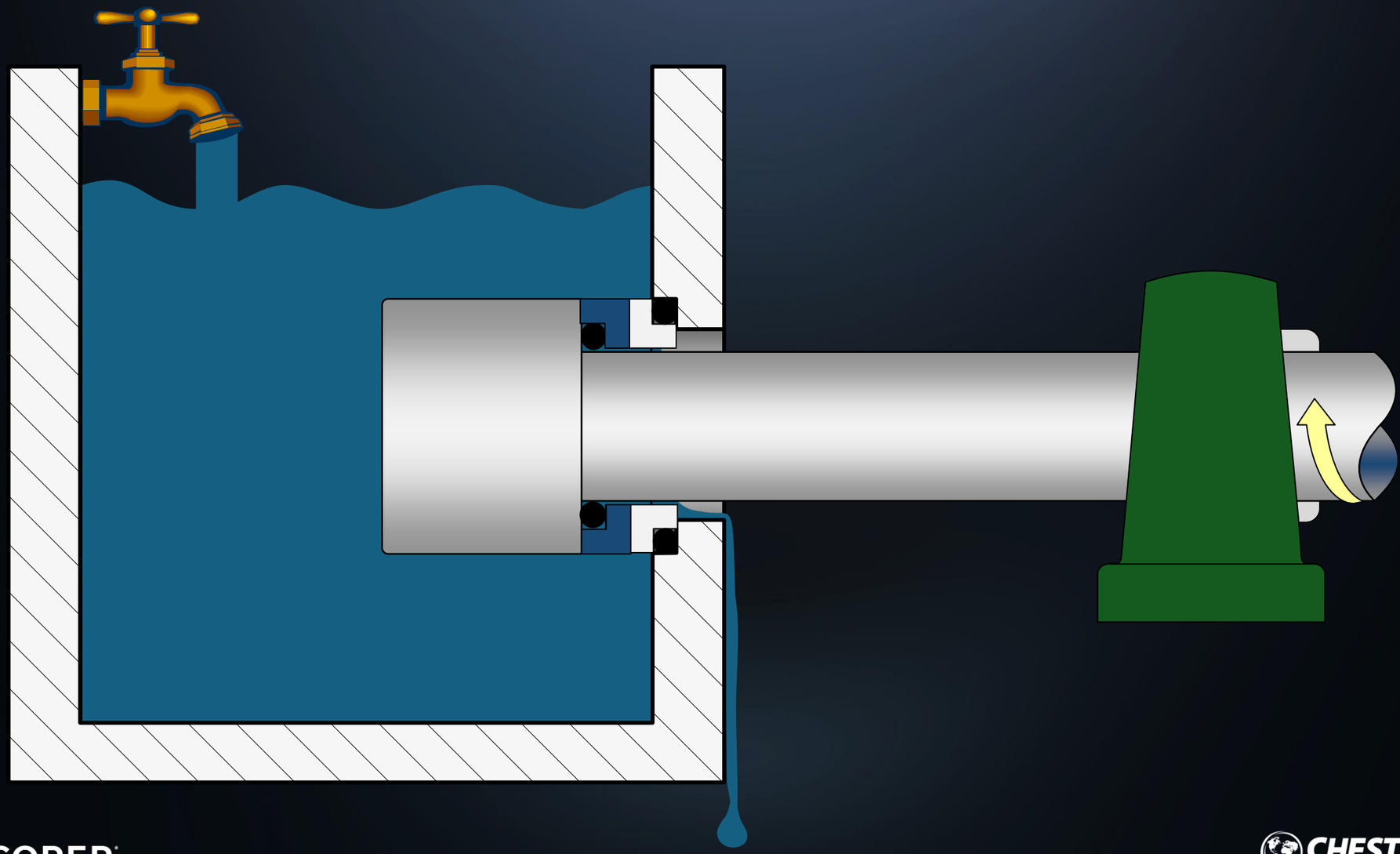
Les Faces



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

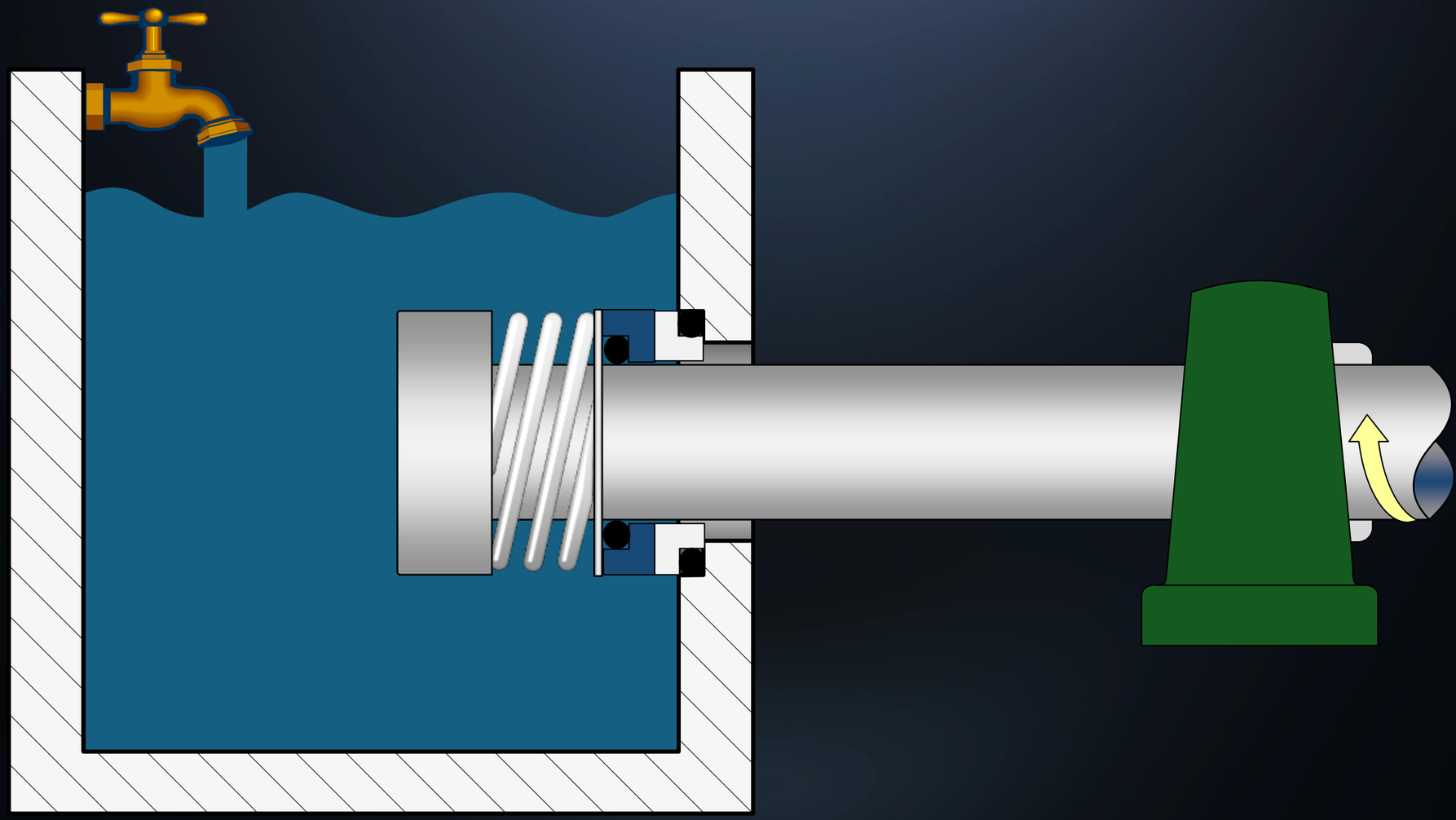
Les joints Secondaires



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

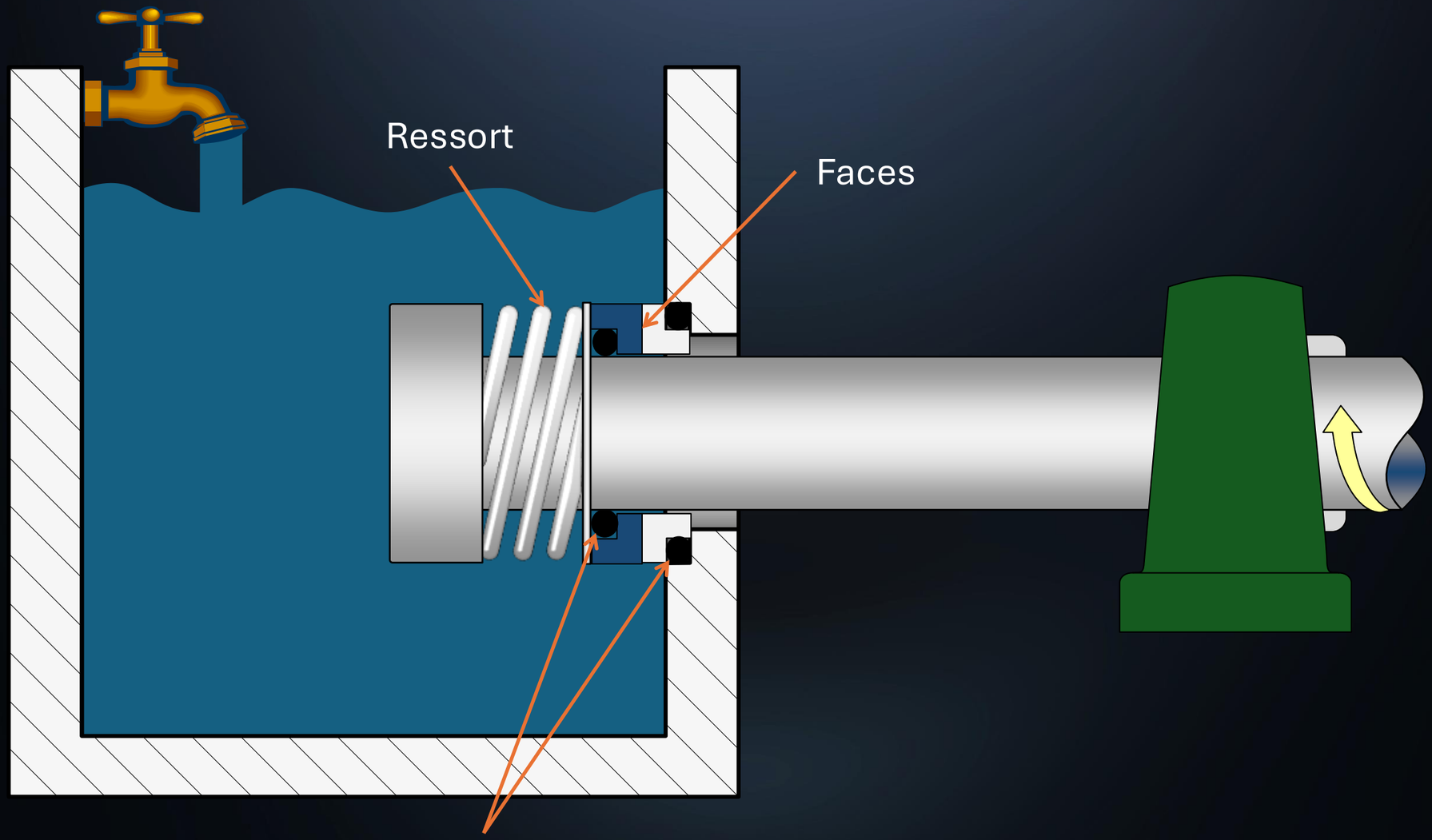
Ressort



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

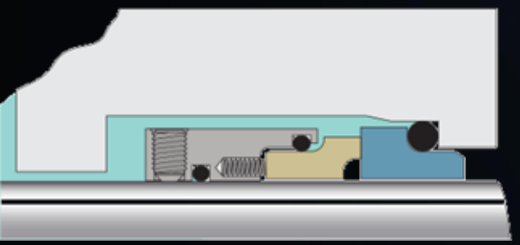
Eléments de la Garniture Mécanique



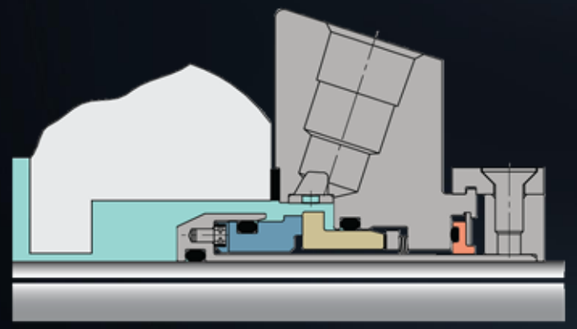
SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

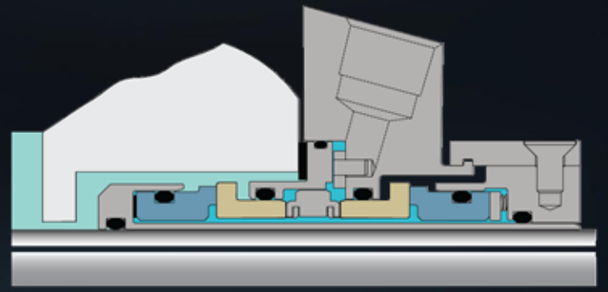
Les différents types de garnitures mécaniques



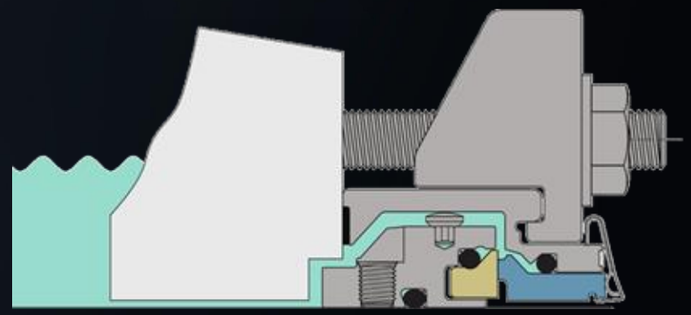
Composant



Cartouche simple



Cartouche double



Sécable

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Tresse Vs Garniture mécanique

Critère	Tresse	Garniture mécanique
Fuite	Fuite con généraler	/h)
Coût initial	Faible (€)	à €€€)
Durée de vie	6 à 18 mo	ne pratique)
Usure de la chemise	Oui — us l'arbre/ch	tact avec l'arbre
Réglage	Régulier -	s installation
Fluides dangereux	Non reco	uble)
Installation	Simple, rapide	Requiert précision
Énergie consommée	Élevée (friction importante)	Faible (film lubrifiant)

Conclusion :
La tresse reste pertinente pour les applications simples, rustiques et économiques.

La garniture mécanique s'impose dès que la criticité, l'environnement ou la réglementation l'exige.

Economies d’énergie

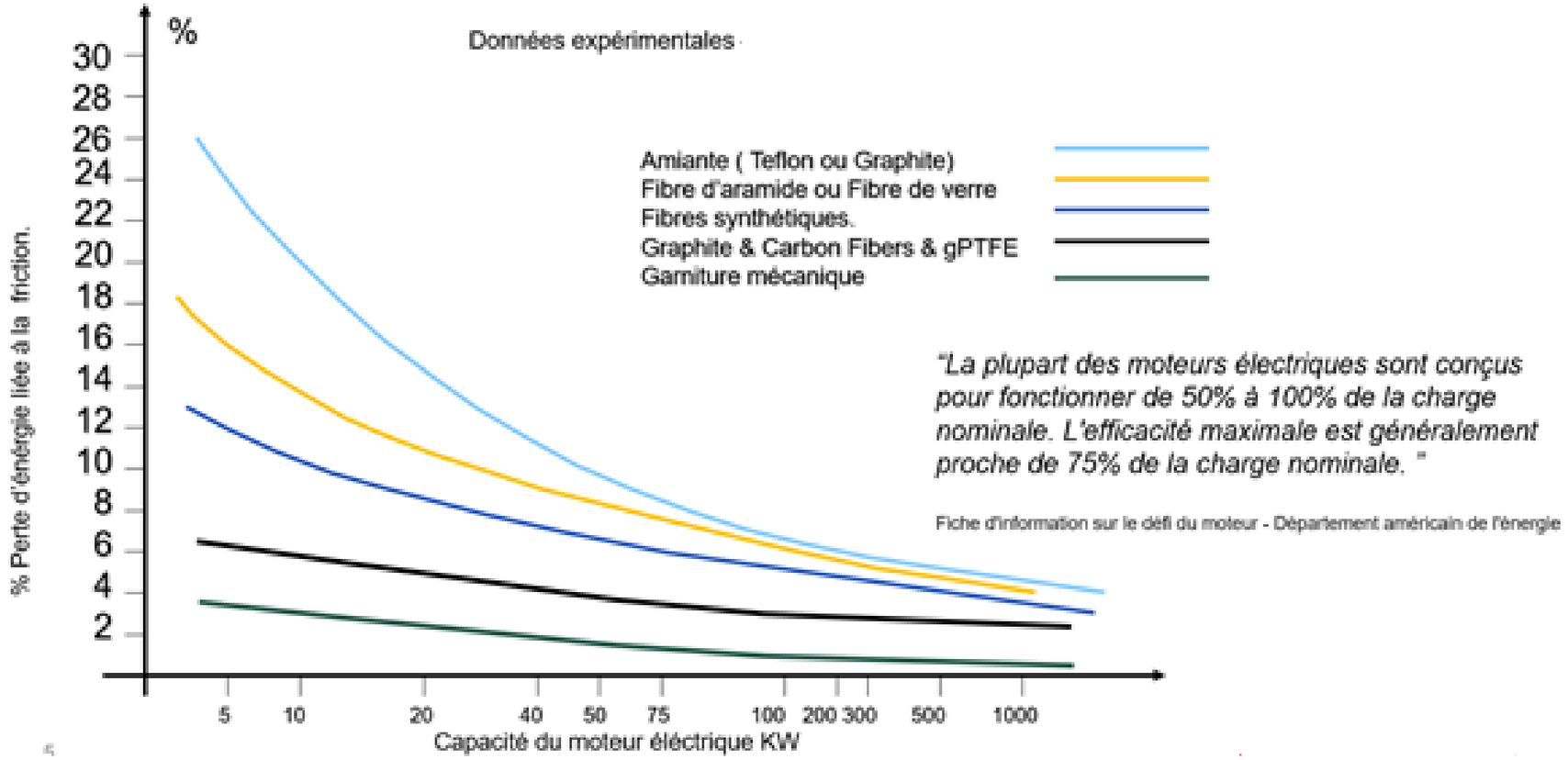
SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Economies d’énergie…. Le coût caché des tresses….

Garniture mécanique	Tresse mal réglée
Film lubrifiant entre les faces → friction minimale	**<u>Fouloir trop serré</u>** → friction élevée → chaleur excessive Surconsommation d’énergie **<u>Fouloir désserré</u>** → fuite excessive → perte de produit

Pertes de puissance liée à l’utilisation des tresses



“La plupart des moteurs électriques sont conçus pour fonctionner de 50% à 100% de la charge nominale. L’efficacité maximale est généralement proche de 75% de la charge nominale. ”

Fiche d'information sur le défi du moteur - Département américain de l'énergie

Changer une tresse pour une garniture mécanique, ce n'est pas une dépense — c'est un investissement qui se rentabilise en quelques mois et génère des économies durables.

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

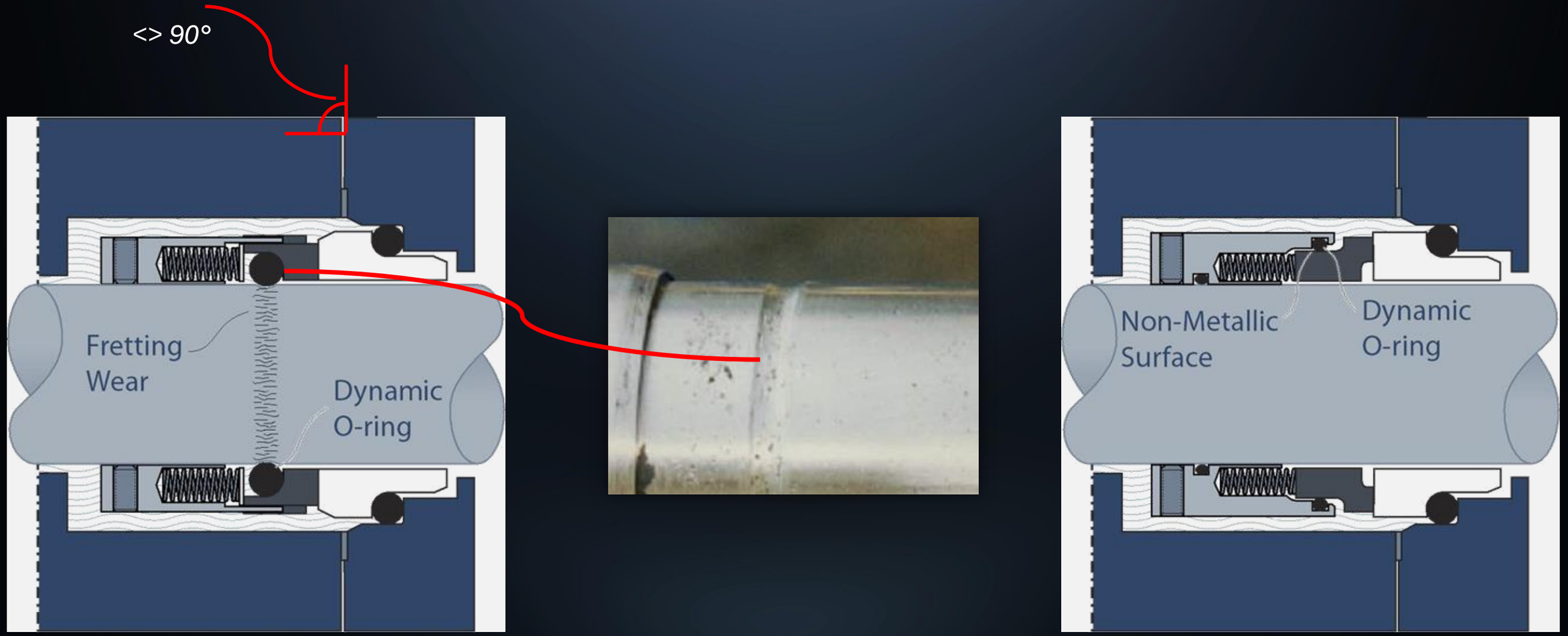
CHESTERTON
Global Solutions, Local Service.

Maitrise de l’usure des chemises – arbres de pompes

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Maitriser l’usure des chemises/arbres de pompes

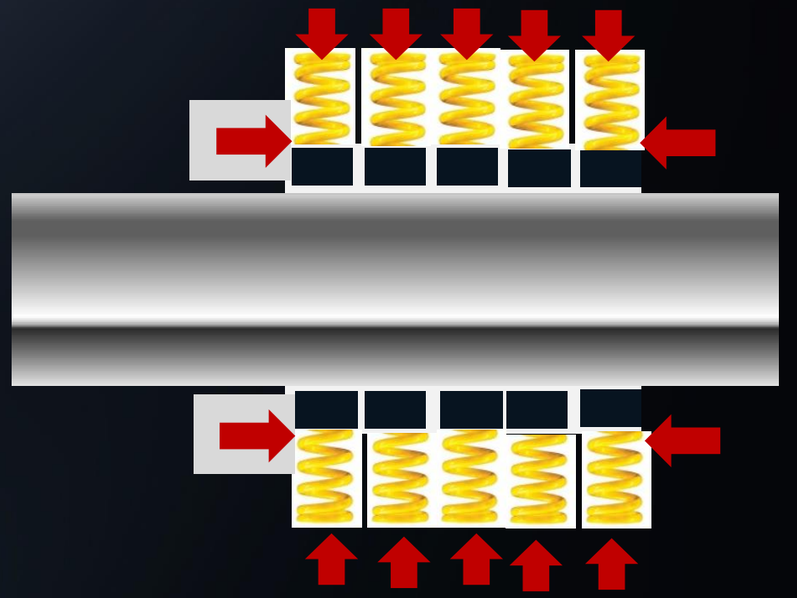


SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Maitriser l’usure des chemises/arbres de pompes

Les fibres d’Aramide fournissent La resilience



Live Loading Interne
Moins de resserrage

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Arrosage – bague séparatrice de solides

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Systèmes de lubrification

Toutes les mesures qui peuvent être prises pour améliorer l'environnement de l’étanchéité fonctionnent pour:

Réduire/augmenter la température

Réduire/augmenter la pression

Mettre en mouvement le fluide

Combinaison des mesures ci-dessus

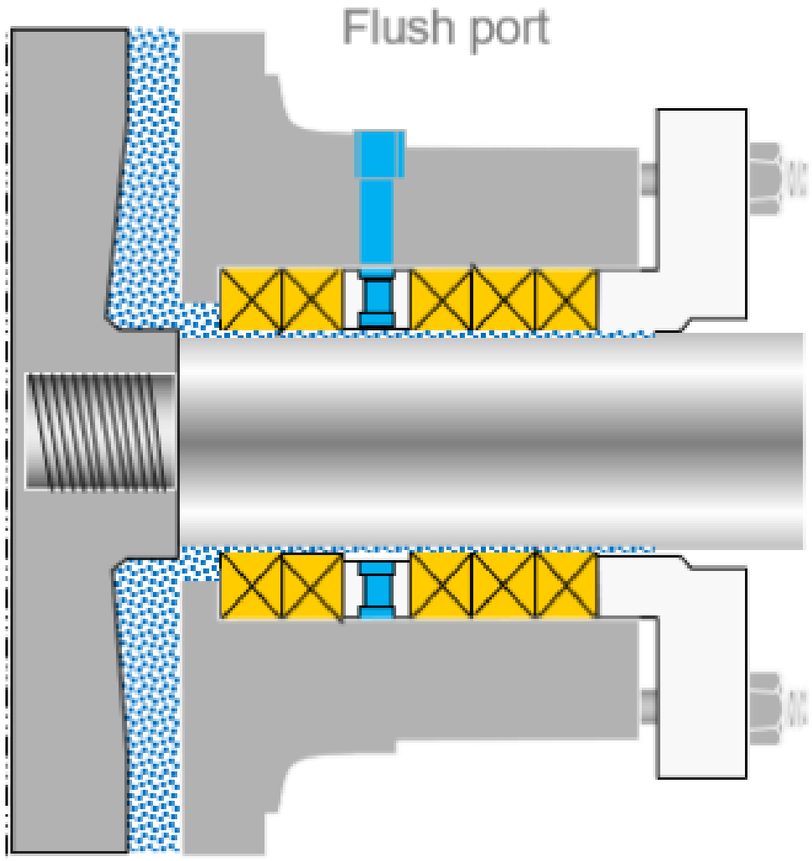
Normes et désignations:

DIN /ISO 5199 VDMA 24297
API 610 (American Petroleum Institute)

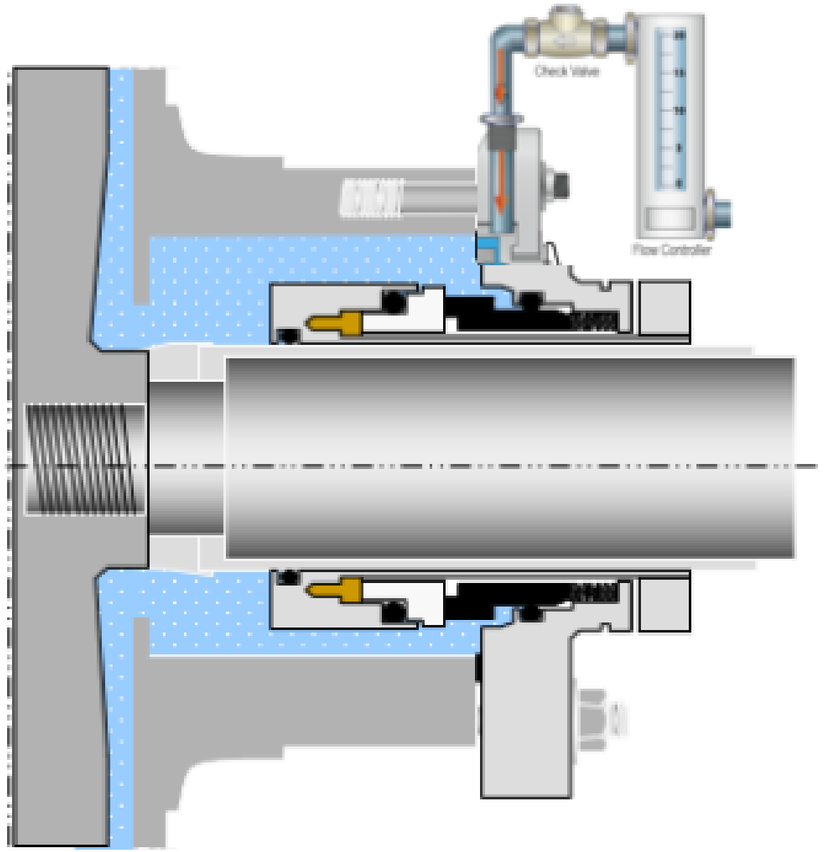
SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Configurations

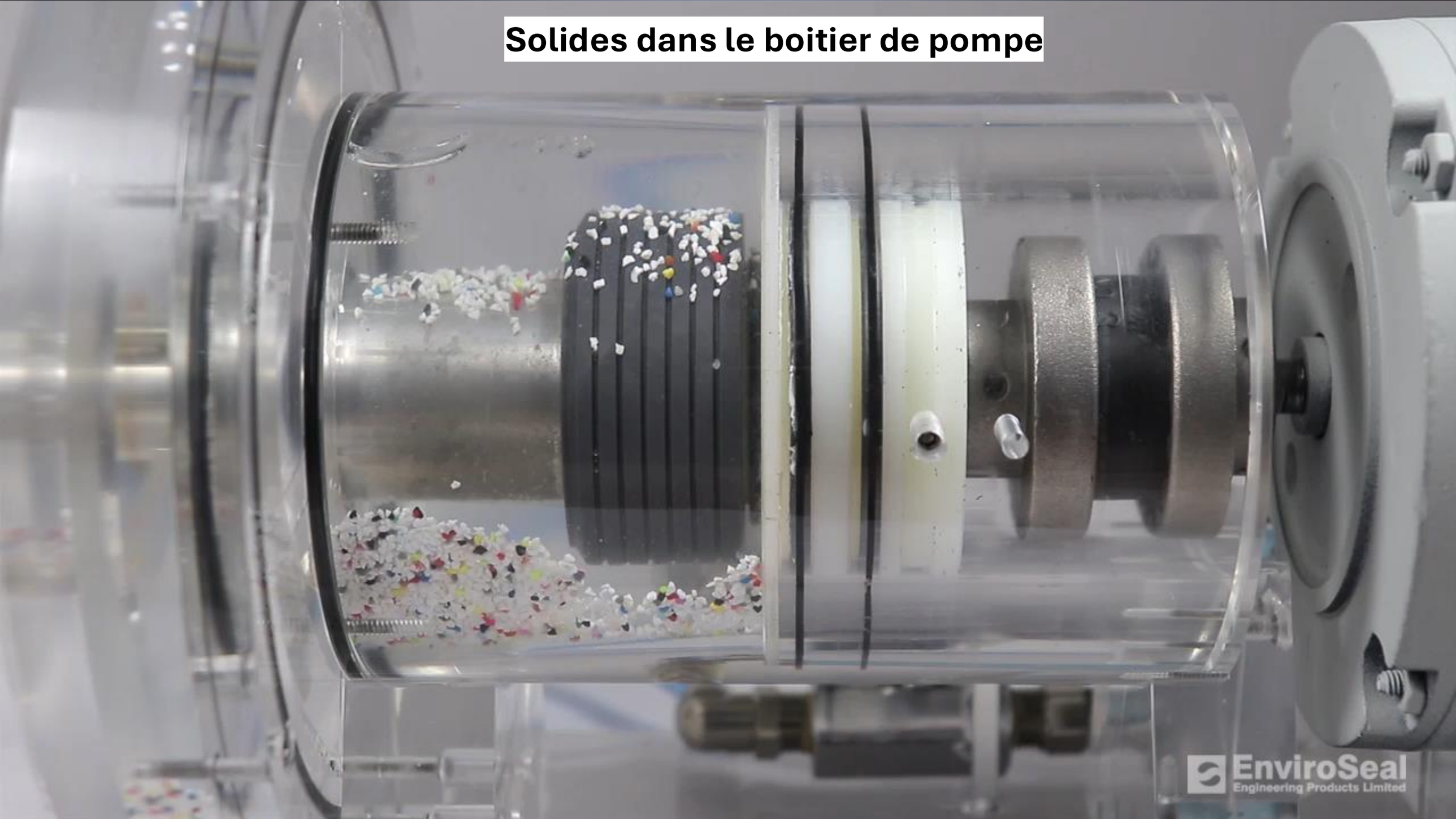


Tresses

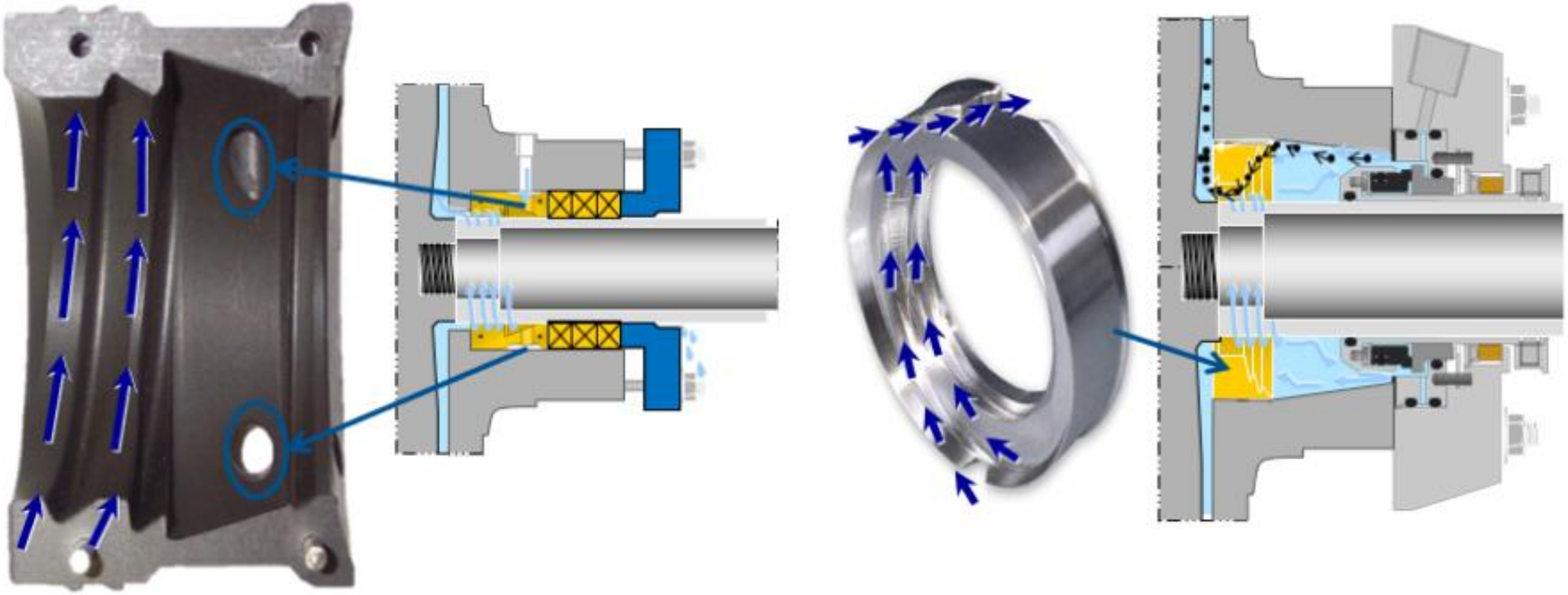


Garniture mécanique

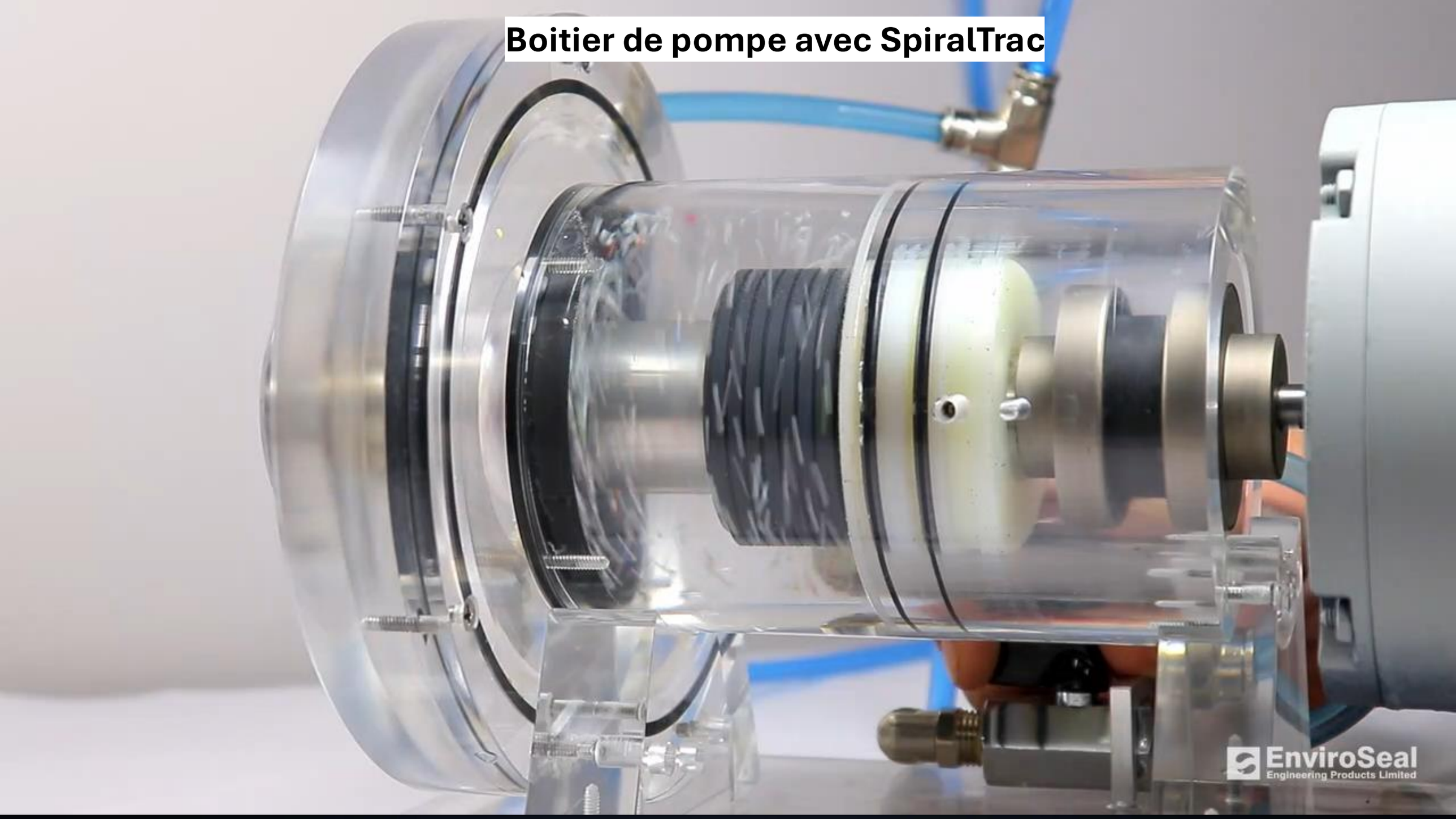
Solides dans le boitier de pompe



Comment fonctionne-t-il ?



Boitier de pompe avec SpiralTrac



A chaque application sa solution

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

A Chaque application ….. sa solution

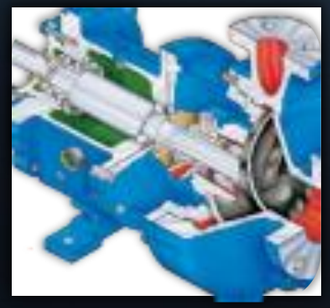
Size

La taille de l’abre ou de la chemise doit etre disponible dans notre gamme

Temperature

La temperature aide a determiner le type d’elastomere de tresse à utiliser

Application



Quel type d’equipement? Fonctionne-t-il continu ou demarrage – arret?

Medium

Resistance chimique des emateriaux a utiliser

Pressure

La pression doit etre dans la plage de limite acceptable par le système d’étanchéité

Speed

La vitesse aide a determiner quel couple de face doit etre utilisé (GM)

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Guide sur la fiabilité et la consommation d'eau dans l'étanchéité des équipements rotatifs

	Solution d'étanchéité	Description	Fiabilité	Consommation d'eau	Prix d'achat
	Tresses standards	Solution simple, faible coût initial, mais nécessitant beaucoup d'entretien. Idéale pour les points non critiques	⚙	💧💧💧💧	€
	Tresses hautes performances	Améliore le MTBR. Moins de réglages, meilleur contrôle des fuites. Première optimisation des coûts d'exploitation sans investissements importants.	⚙⚙	💧💧💧	€
	Dualpac® + Spiraltrac	Réduction de la consommation d'eau, allongement de la durée de vie, nettoyage interne. Assure un contrôle passif des fuites et une meilleure efficacité du système.	⚙⚙⚙	💧💧	€€
	Garniture mécanique Simple/Double	Conception robuste. Moins d'eau de lavage. Réduit l'usure et permet une meilleure étanchéité.	⚙⚙⚙	💧💧	€€
	Garniture mécanique avec Spiraltrac	Une avancée décisive en matière d'étanchéité. Moins de fuites, plus de fiabilité. Cette solution facilite la maintenance des équipements de grande taille.	⚙⚙⚙⚙	💧	€€€
	Garniture Double et Plan API	Fiabilité et contrôle maximal. Surveillance active, sécurité, conformité réglementaire. Pour les services critiques ou à haut risque.	⚙⚙⚙⚙⚙		€€€€€

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

⚙ 💧 € Note de 1 à 5, 1 étant la note minimale et 5

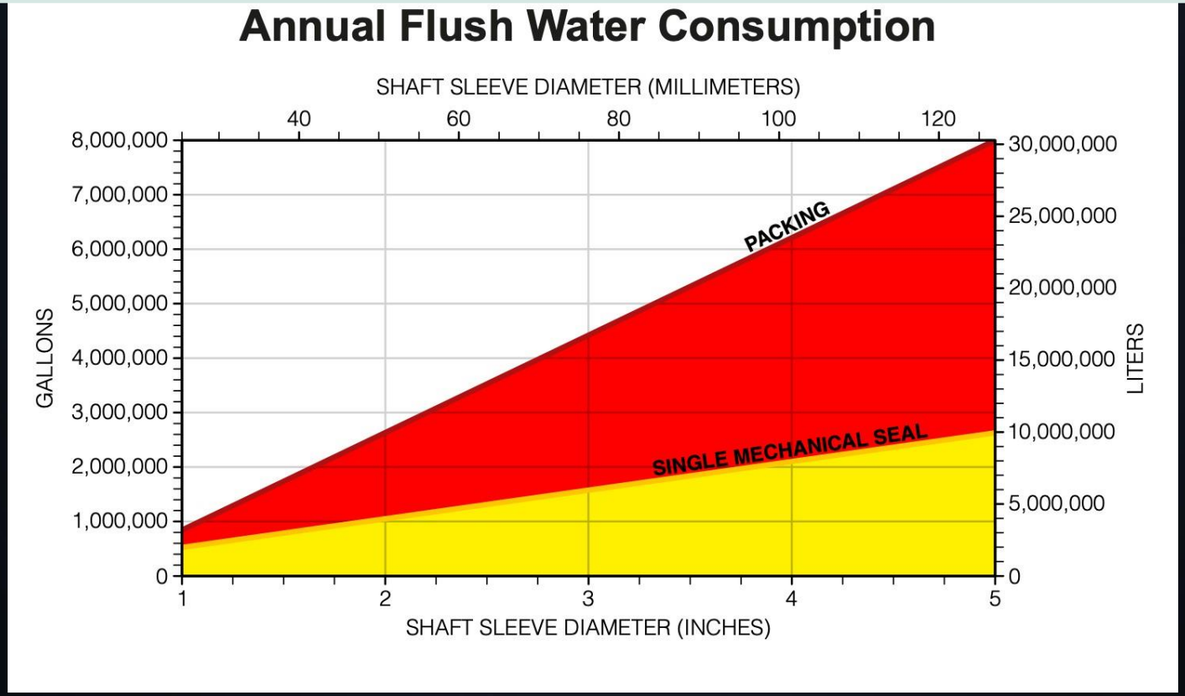
CHESTERTON
Global Solutions, Local Service.

Fiabilisation et Tribologie

La **fiabilité d'un système d'étanchéité** dépend de la **tribologie**, c'est-à-dire de la relation entre le **frottement, l'usure et la lubrification** au sein de l'ensemble du système d'étanchéité.

Plus le système génère de frottements, plus nous aurons besoin de lubrification (apport de produit de rinçage).
Nous devons veiller à ce que la lubrification soit assurée et que le fluide soit propre et à température adéquate afin de prolonger la durée de vie (MTBF) du système.

Pour réduire les frottements, il faut utiliser **des conceptions et des matériaux** spécialement conçus à cet effet.



SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

Conclusion

1	Choisir la bonne technologie d'étanchéité, c'est protéger son équipement et réduire ses coûts de maintenance.
2	La garniture mécanique, bien choisie, remplace avantageusement la tresse dans la grande majorité des cas.
3	Chaque euro investi en étanchéité performante génère un retour mesurable : énergie, maintenance, durée de vie.
4	Maîtriser l'environnement de l'étanchéité (arrosages, Spiral Trac) démultiplie les bénéfices.

QUESTIONS ?

SNECOREP
LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

CHESTERTON
Global Solutions, Local Service.

CALENDRIER À VENIR

Assemblée Générale 04/06

Cocktail déjeunatoire

AG

- 2 interventions sur le thème de l'eau avec Simon PORCHER et Dominique GAUTIER

- Election du Président

Et

La soirée des 40 ans

Matinée Thématique 30/09

DANFOSS :

Enjeux actuels et futurs liés à la performance énergétique et à l'optimisation des installations.

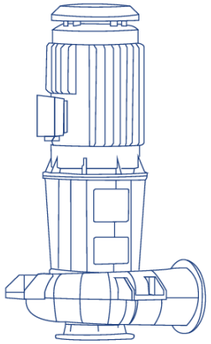
CALENDRIER À VENIR

Commission Label
14/10/2026

(Dépôt dossier avant fin 08/2026)

Rencontre en PACA – CANAL de PROVENCE

**/10/2026 – Matin



SNECOREP®

LE SYNDICAT DES PROFESSIONNELS DU POMPAGE

MERCI DE VOTRE ATTENTION