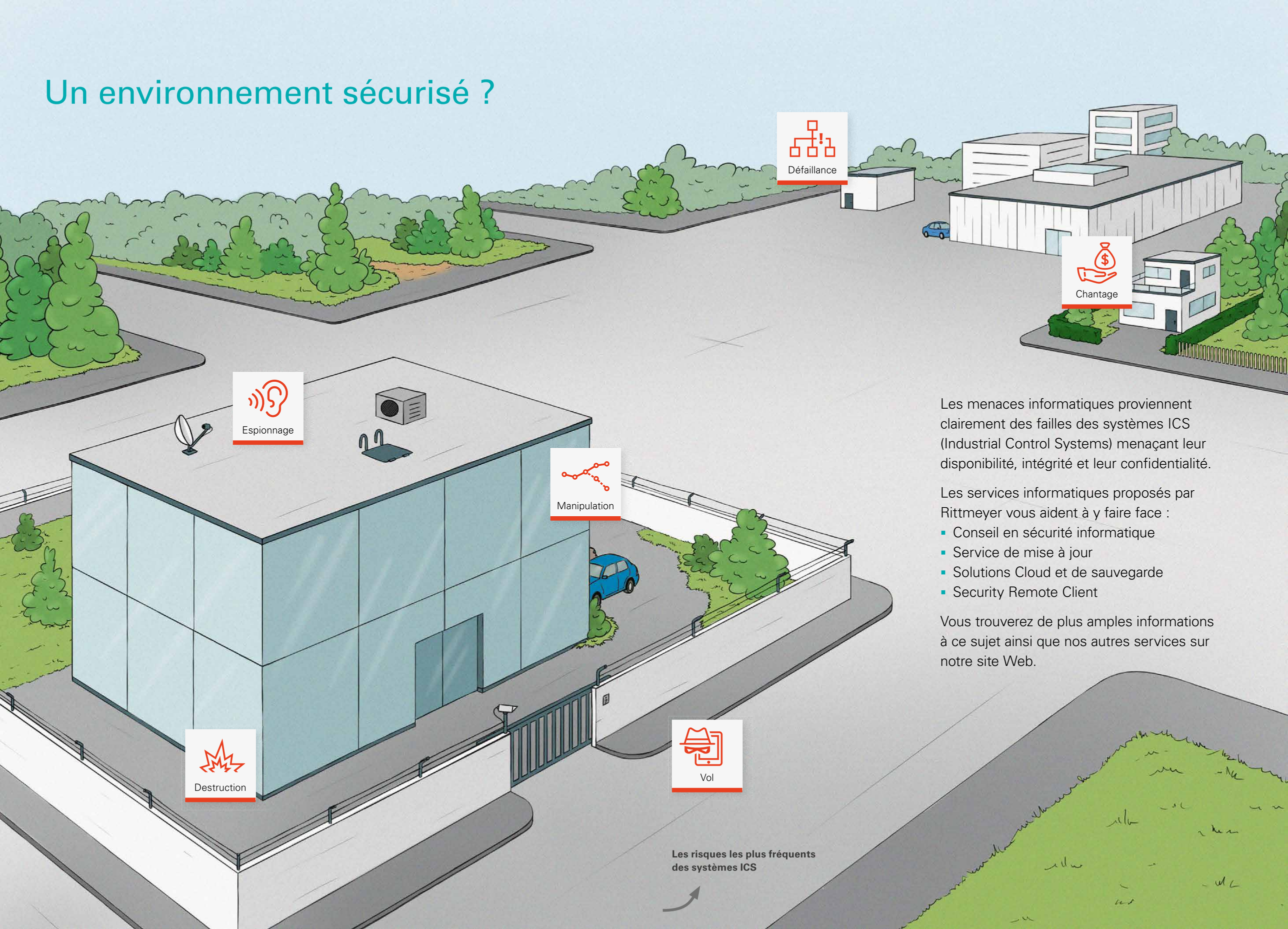
rittmeyer
BRUGG

FAILLES DE SÉCURITÉ DANS LES INFRASTRUCTURES CRITIQUES

Les risques les plus fréquents liés aux systèmes ICS (Industrial Control Systems)

Un environnement sécurisé ?



Les menaces informatiques proviennent clairement des failles des systèmes ICS (Industrial Control Systems) menaçant leur disponibilité, intégrité et leur confidentialité.

Les services informatiques proposés par Rittmeyer vous aident à y faire face :

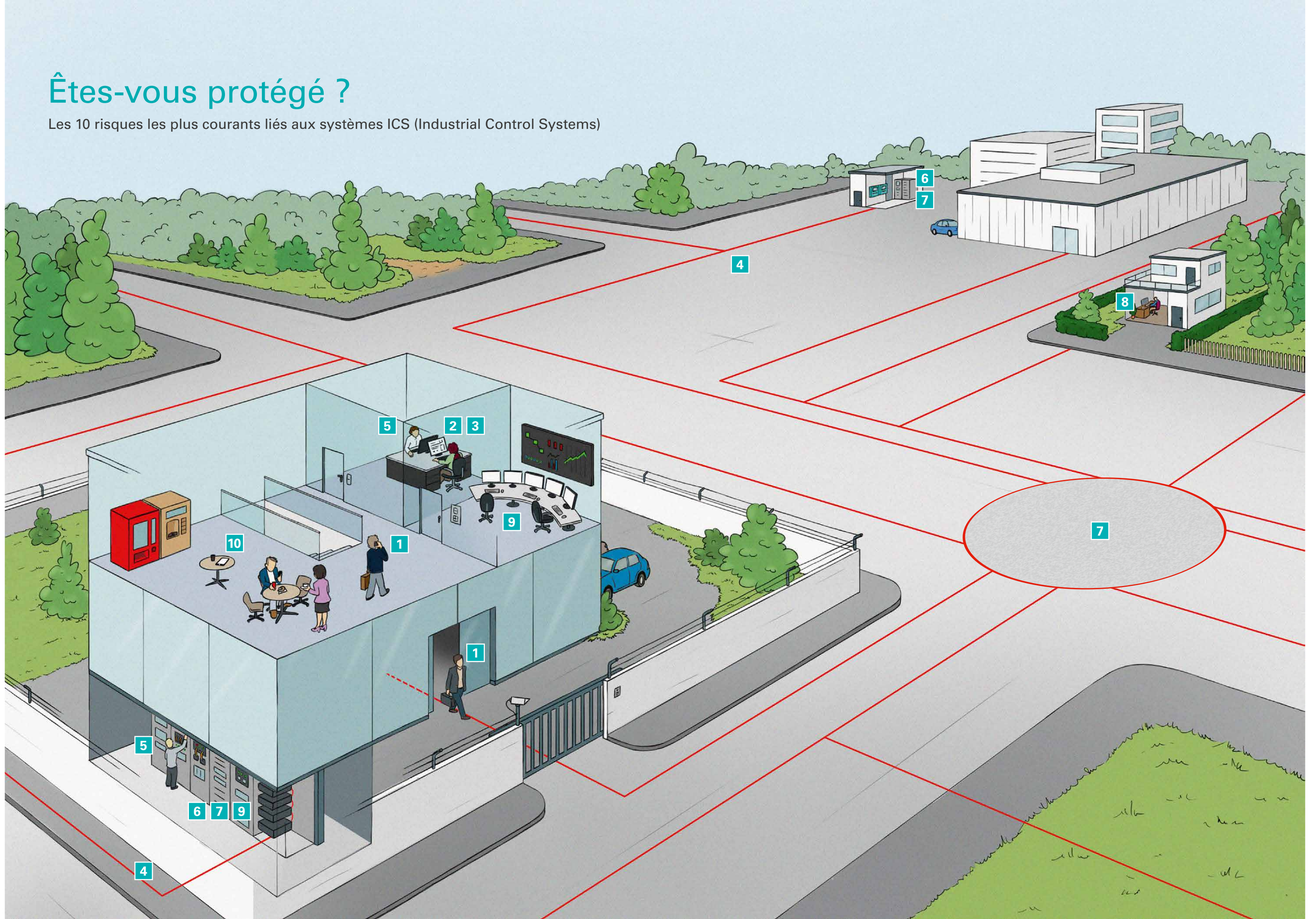
- Conseil en sécurité informatique
- Service de mise à jour
- Solutions Cloud et de sauvegarde
- Security Remote Client

Vous trouverez de plus amples informations à ce sujet ainsi que nos autres services sur notre site Web.

Les risques les plus fréquents des systèmes ICS

Êtes-vous protégé ?

Les 10 risques les plus courants liés aux systèmes ICS (Industrial Control Systems)



1 Social Engineering

L'ingénierie sociale (‹ Social Engineering ›) renvoie à la manipulation des personnes afin d'obtenir des informations cruciales et détourner les dispositifs de sécurité. Les personnes sont manipulables et par conséquent le maillon faible dans la chaîne de sécurité.

Protection

- Formation de sensibilisation à la sécurité
- Réglementations de sécurité
- Contrôles d'accès
- Prise de conscience
- Définition de procédures d'alarme

2 Lecteurs mobiles : infiltration de logiciels malveillants

Les employés se servent de lecteurs mobiles et de matériel externe, comme les clés USB, en parallèle à l'utilisation du réseau bureautique et ICS, sans oublier l'usage privé courant.

Protection

- Protection technique
- Protection antivirus
- Sauvegarde des données
- Administration des habilitations
- Renforcement de l'ordinateur
- Réglementations pour les utilisateurs

3 Internet/Intranet : contamination avec des logiciels malveillants

Les navigateurs et les clients de messagerie sont le plus souvent connectés à Internet.

Protection

- Protection antivirus
- Mises à jour logicielles
- Sauvegarde des données
- Responsabilités
- Administration des habilitations
- Renforcement de l'ordinateur
- Réglementations pour les utilisateurs

4 Accès de télémaintenance

Les installations ICS impliquent très souvent des accès externes pour la maintenance. Pour ce faire, on s'appuie sur des accès standard avec des mots de passe par défaut, voire de mots de passe à codage fixe. Tout ceci facilite les intrusions par les cybercriminels.

Protection

- Pare-feu
- Codage SSL/TLS
- Clés pré-partagées
- Certificats
- Accès personnalisés
- Audits
- Modification des mots de passe par défaut
- Segmentation granulaire des réseaux
- Codage des données sensibles
- Autorisation des accès de télémaintenance par le personnel interne
- Protocoles des accès distants

5 Comportement humain et sabotage

L'environnement de travail du personnel ICT prend une position bien particulière au centre de la sécurité informatique. Les manipulations dans ces environnements se produisent de manière consciente et inconsciente.

Protection

- Protection physique
- Formations
- Réglementations pour les utilisateurs
- Administration des habilitations
- Mise en place du principe ‹ Need to know ›
- Surveillance automatique des états du système et des configurations

6 Composants de commande connectés à Internet

Souvent les composants ICS comme les API sont directement connectés à Internet (Internet of Things, IoT).

Protection

- Pare-feu
- Mises à jour logicielles
- Modification des mots de passe par défaut

7 Comportement inadapté et dangers imminents

Il est impossible d'exclure les erreurs logicielles dans des composants de sécurité ainsi que dans des composants ICS, ni les défaillances matérielles et les coupures de réseaux.

Protection

- Protection physique
- Systèmes redondants
- Appareils de rechange et de remplacement
- Maintenance
- Mise en œuvre d'un plan de secours
- Utilisation d'interfaces standardisées

8 Piratage d'extranet et des composants Cloud

Les services informatiques traditionnels ont l'habitude de sous-traiter les composants informatiques. Cette pratique gagne de plus en plus les systèmes ICS.

Protection

- Accès VPN
- Fournisseurs certifiés
- Systèmes redondants
- Accords sur les niveaux de service
- Mécanismes cryptographiques

9 Attaque (D)DoS

La communication entre les composants ICS passent à la fois par les réseaux filaires et Wifi. Lorsque les connexions sont perturbées, les données de mesure et de commande risquent d'être mal transmises. Un composant peut se retrouver surcharger par des requêtes trop abondantes l'empêchant de transmettre une réponse à temps.

Protection

- Détection des intrusions
- Connexions redondantes grâce à différents protocoles
- Connexions filaires dédiées aux fonctions critiques
- Renforcement des accès au réseau

10 Environnement de production : piratage des smartphones/tablettes

L'affichage et la modification des paramètres de service et de production pour les composants ICS passent de plus en plus par les smartphones ou les tablettes.

Protection

- Accès VPN
- Réglementations pour les utilisateurs
- Utilisation de centres d'application certifiés
- Administration des habilitations
- Gestion des terminaux mobiles
- Fin des accès directs aux systèmes ICS depuis une application

Rittmeyer, une société du BRUGG GROUP, développe et fournit des solutions de conduite et de mesure prêtes à l'emploi dédiées à l'approvisionnement en eau et en énergie, aux centrales hydrauliques et aux stations d'épuration. Depuis 1904, le nom Rittmeyer est synonyme de produits et de services haut de gamme. Rittmeyer se positionne comme partenaire auprès de ses clients et les accompagne pendant toute la durée de vie de leurs installations – de la conception à la formation en passant par la planification, la mise en service, l'installation et de nombreux services. Avec six succursales, un bureau de vente et des revendeurs dans plus de 25 pays, Rittmeyer est présent dans le monde entier.

www.rittmeyer.com

rittmeyer
BRUGG

Rittmeyer AG
Inwilerriedstrasse 57
BP 1660
CH-6341 Baar
+41 41 767 10 00
security@rittmeyer.com

82824.1.F | 1804 ERN
Sous réserve de modifications