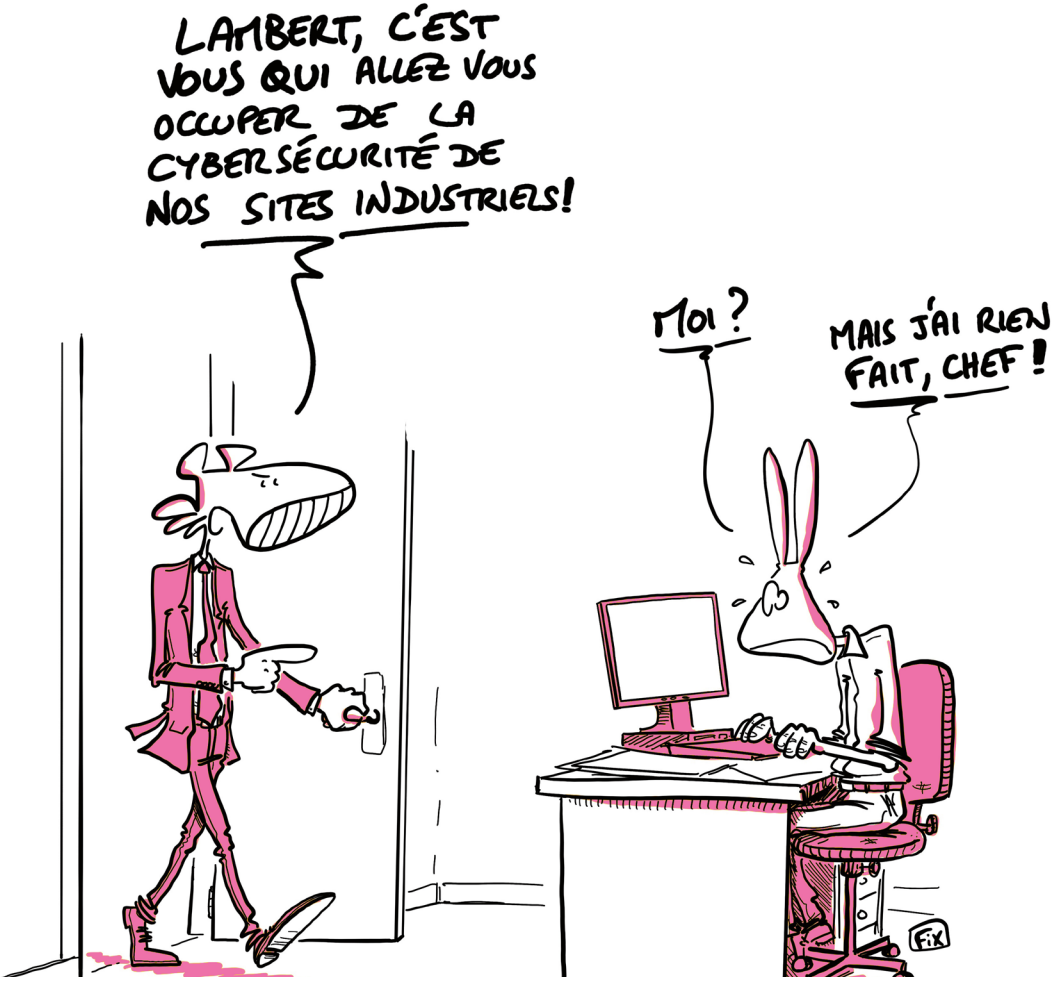
Volet 3

Guide de survie du RSSI en environnement industriel

Glossaire


LAMBERT, C'EST VOUS QUI ALLEZ VOUS OCCUPER DE LA CYBERSÉCURITÉ DE NOS SITES INDUSTRIELS!
MOI ?
MAIS J'AI RIEN FAIT, CHEF !
FIX

Les mots de la présidente

Les entreprises ont besoin de cybersécurité pour protéger leurs activités, leurs données mais aussi pour s'inscrire dans les exigences de confiance vis-à-vis des solutions numériques, qu'ont désormais les utilisateurs internes et externes, clients et partenaires, au-delà d'une expérience utilisateur de qualité.

La cybersécurité est en train de vivre une évolution majeure qui prend en compte d'un côté l'évolution croissante des menaces et de l'autre la transformation des architectures, des solutions numériques et des organisations qui les conçoivent.

Ceux qui conduisent la cybersécurité ont besoin de partager des pratiques, des méthodes, des expériences et des informations. La compréhension des risques et le renseignement sur les menaces sont essentiels. La diversité des métiers et des organisations des membres du CESIN est une opportunité pour des échanges et un travail en réseaux fructueux. Cette coopération est l'ambition du CESIN, elle s'opère dans la confiance et la convivialité. Elle se veut pragmatique et efficace, au service des membres et de leur entreprise. Elle constitue un réel atout dans les stratégies de défense.

Les Labs sont un des outils que le CESIN met à disposition de ses membres. Réunis en petit groupe de travail de 10/15 personnes, les membres entreprennent une démarche exploratoire, de recherche ou d'approfondissement d'une question ciblée. Ils partagent leur expérience pour répondre à une problématique précise et dans un délai convenu. Les résultats produits par les labs peuvent prendre différentes formes et sont mis à disposition de l'ensemble des membres.

5S (OT)

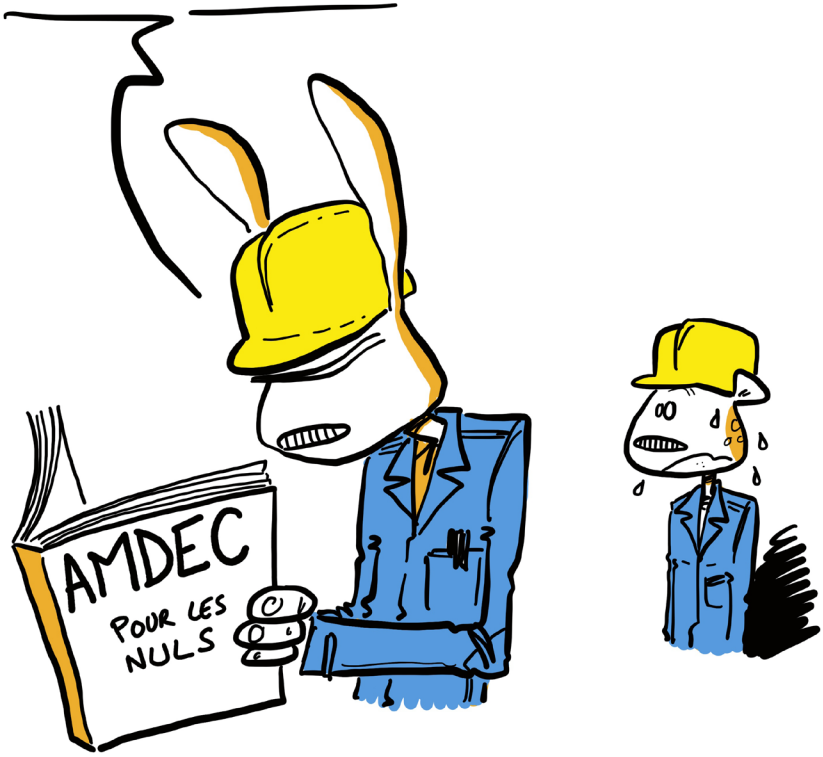
Technique de gestion japonaise visant à l'amélioration continue des tâches effectuées dans les usines. Souvent traduite en français par le mot **ORDRE** : (Ordonner, Ranger, Dépoussiérer et Découvrir les anomalies, Rendre évident et Être rigoureux). N'en concluez pas que les usines qui ne l'appliquent pas sont désordonnées, poussiéreuses et que l'on y manque de rigueur.

Actionneur (OT)

Périphérique relié à un automate, produisant un effet physique participant au process industriel. Il peut par exemple démarrer ou arrêter une pompe. C'est la présence de l'actionneur qui fait toute la différence entre l'IT et l'OT. Dans l'OT, on peut produire un effet physique.


LES CHOSES DANS L'O.R.D.R.E.(*), PETIT SCARABÉE.
JE VÉNÈRE TA SAGESSE, Ô VIEUX SCARABÉE.
FiX

LAISSEZ-MOI VÉRIFIER, LAMBERT, MAIS JE CROIS QUE RIEN NE M'EMPÊCHE DE VOUS DÉSIGNER COMME POINT DE DÉFAILLANCE...



A

AGV (OT)

Automatic Guided Vehicle. Voir VGA.

AMDEC (OT)

Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité. Technique d'analyse, en maintenance prédictive, permettant de détecter à l'avance les points faibles d'un système, afin de l'améliorer ou de prévoir les pannes à venir. Voir également **HAZOP** ; le choix de AMDEC ou HAZOP relève de la guerre de religion. N'allez surtout pas vous imaginer que le risque cybersécurité est prévu a priori dans les analyses de risques métier.

Analogique (OT)

S'oppose à Numérique. Se dit de signaux qui varient en amplitude, phase, fréquence, etc. Bref, tout le contraire des 0 et des 1 chers aux informaticiens.

Un signal analogique peut être utilisé par exemple pour récupérer une température ou une pression.

A

API (OT)

Si pour le RSSI, l'API est une interface de programmation (Application programming Interface), pour l'automaticien il s'agit d'un Automate Programmable Industriel... aussi connu sous le nom de PLC (Programmable Logic Controller). Il envoie des ordres vers les actionneurs à partir de données d'entrées (issues des capteurs), de consignes et d'un programme logique.

ATEX (OT)

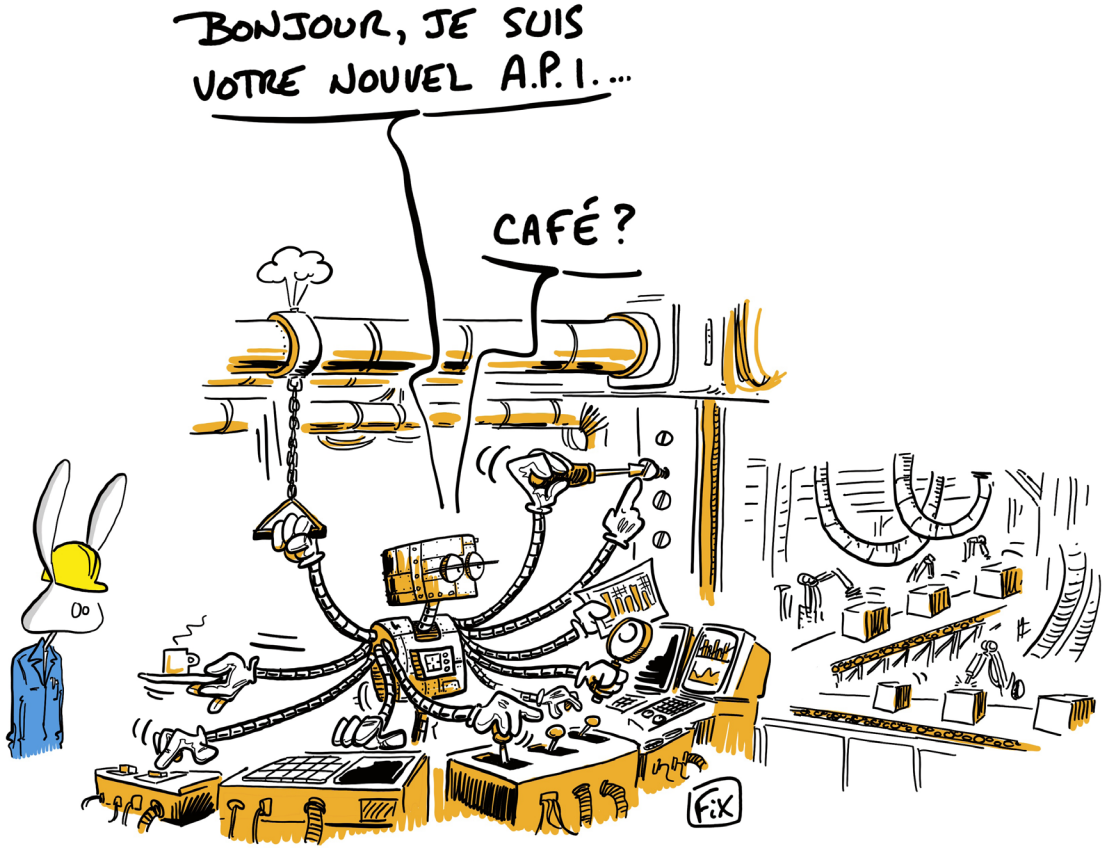
Atmosphère explosive. Normalement on la repère au stress des salariés à la vue du visiteur qui allume sa cigarette, ou à la signalétique réglementaire.On ne vous y invitera que si vous avez l'habilitation ad hoc.

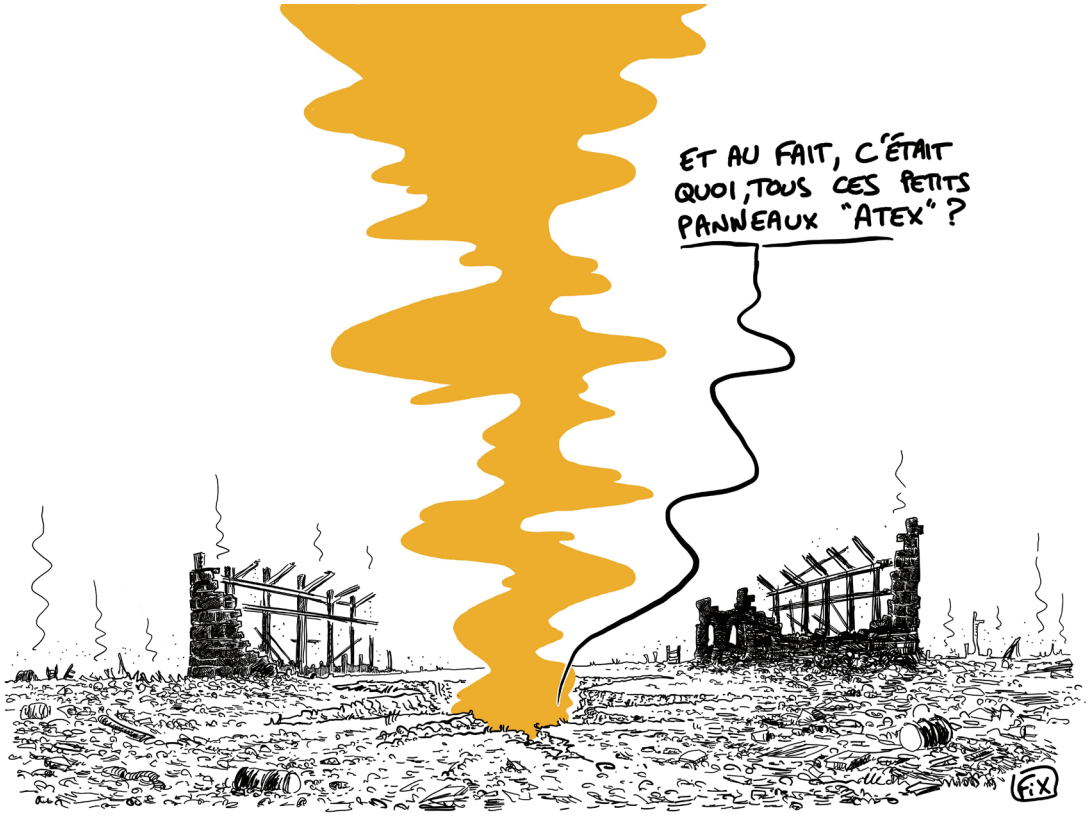
Automate (OT)

Voir API.

Automaticien (OT)

La personne qui a la lourde tâche de programmer et de maintenir les automates en état de fonctionnement. C'est le premier à convaincre du risque cybersécurité.


BONJOUR, JE SUIS VOTRE NOUVEL A.P.I...
CAFÉ ?
FiX


ET AU FAIT, C'ÉTAIT QUOI, TOUS CES PETITS PANNEAUX "ATEX" ?
FIX

B

Bus de terrain (OT)

Non, il ne s'agit pas de la navette qui circule dans l'usine pour transporter les salariés. Un bus de terrain est une liaison permettant de raccorder un ou des capteur(s) et/ou un ou des actzionneur(s) à un automate.

Historiquement, cette liaison était directement câblée. L'avenir est aux capteurs et aux actionneurs connectés à un réseau IP (voir aussi Protocoles Réseaux), ce qui ne manquera pas de vous amener des problèmes de sécurité supplémentaires.

C

Capteur (OT)

Périphérique capable de traduire une grandeur physique (pression, température, présence...) en une information utilisable par un automate.

Par exemple un capteur peut mesurer le débit instantané d'une pompe.

Le capteur est à l'automate ce que vos yeux, votre nez, vos doigts, vos oreilles et votre goût sont à votre cerveau.

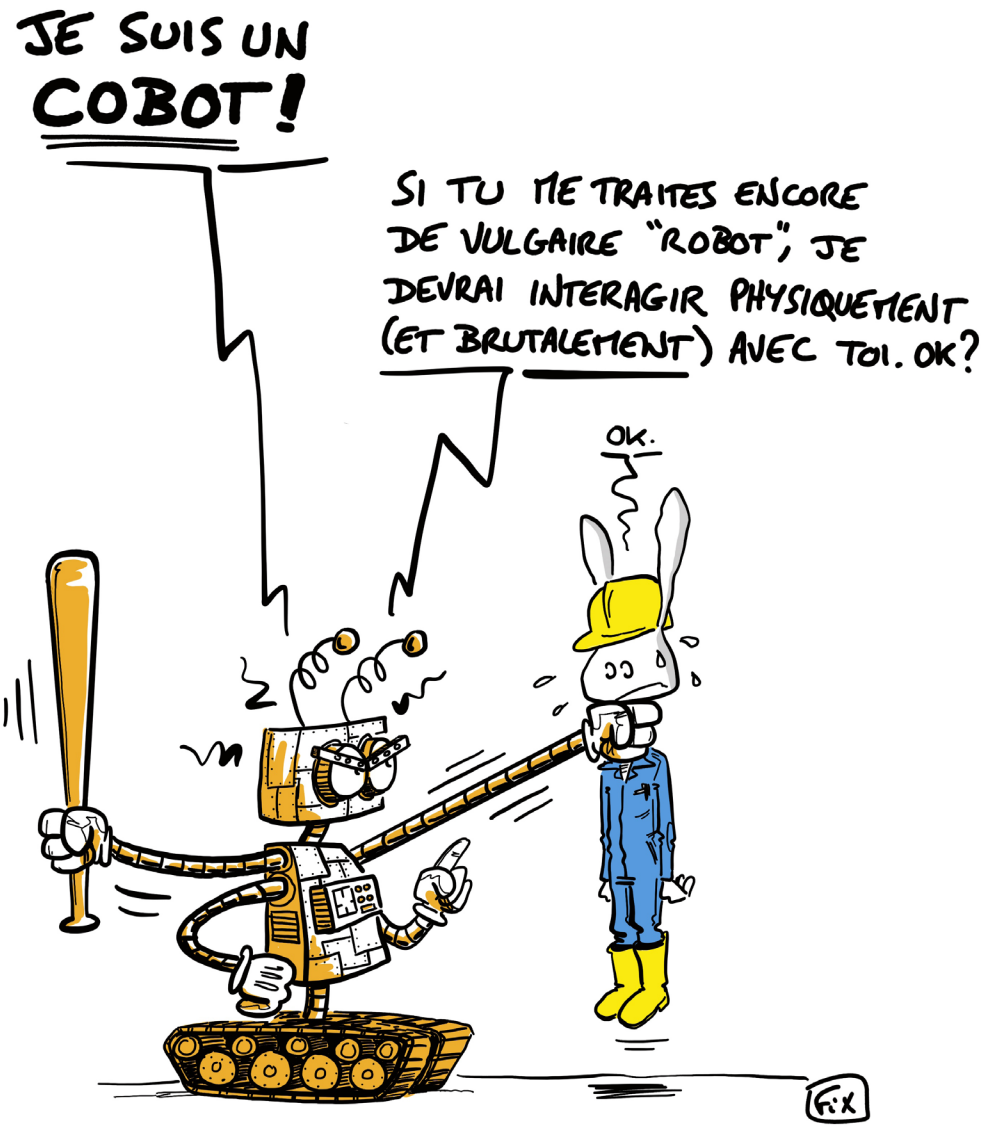
Chien de garde (OT)

Le chien de garde n'est pas le chien du vigile à l'entrée de l'usine.

Dans l'OT, le chien de garde est un dispositif électronique ou logiciel qui permet de définir et de garantir une limite de process. C'est par exemple une protection destinée à redémarrer le système si une action ne se termine pas dans le temps imparti.

Exemple : le chien de garde d'un carrefour à feu, qui passe tous les feux en orange clignotant si deux feux verts incompatibles sont allumés en même temps.


REX ! ON A UN PROCESS EN RADE ! RE.BOOTE LE SYSTÈME !
WOUF !
REBOOT
FiX


JE SUIS UN COBOT!
SI TU ME TRAITES ENCORE DE VULGAIRE "ROBOT", JE DEVRAI INTERAGIR PHYSIQUEMENT (ET BRUTALEMENT) AVEC TOI. OK?
OK.
FIX

C

Cobot (OT)

Plus élaboré qu'un robot, c'est un robot collaboratif. Un robot destiné à interagir physiquement avec des humains dans un espace partagé. Leur programmation permet des usages multiples. Evitez cependant de lui faire un câlin, il n'est pas très réceptif.

Constructeur/ équipementier/éditeur (OT)

Si dans l'IT, on parle généralement de constructeur (matériel) ou d'éditeur (logiciel), dans l 'OT, on parlera généralement d'équipementier, qui fournit les deux.

Contrôle Commande (OT)

Le contrôle commande est -par opposition à la supervision - le fait de piloter un système industriel.

D

DCS (OT)

Distributed Control System.
L'une des appellations d'un système de contrôle industriel. La différence avec un ICS est assez subtile et relève plus des habitudes de vocabulaire que d'une vraie différence (système distribué ou non).

DICT (IT)

Disponibilité / Intégrité / Confidentialité / Traçabilité.

Autant vous le dire tout de suite, vous ne serez jamais d'accord :

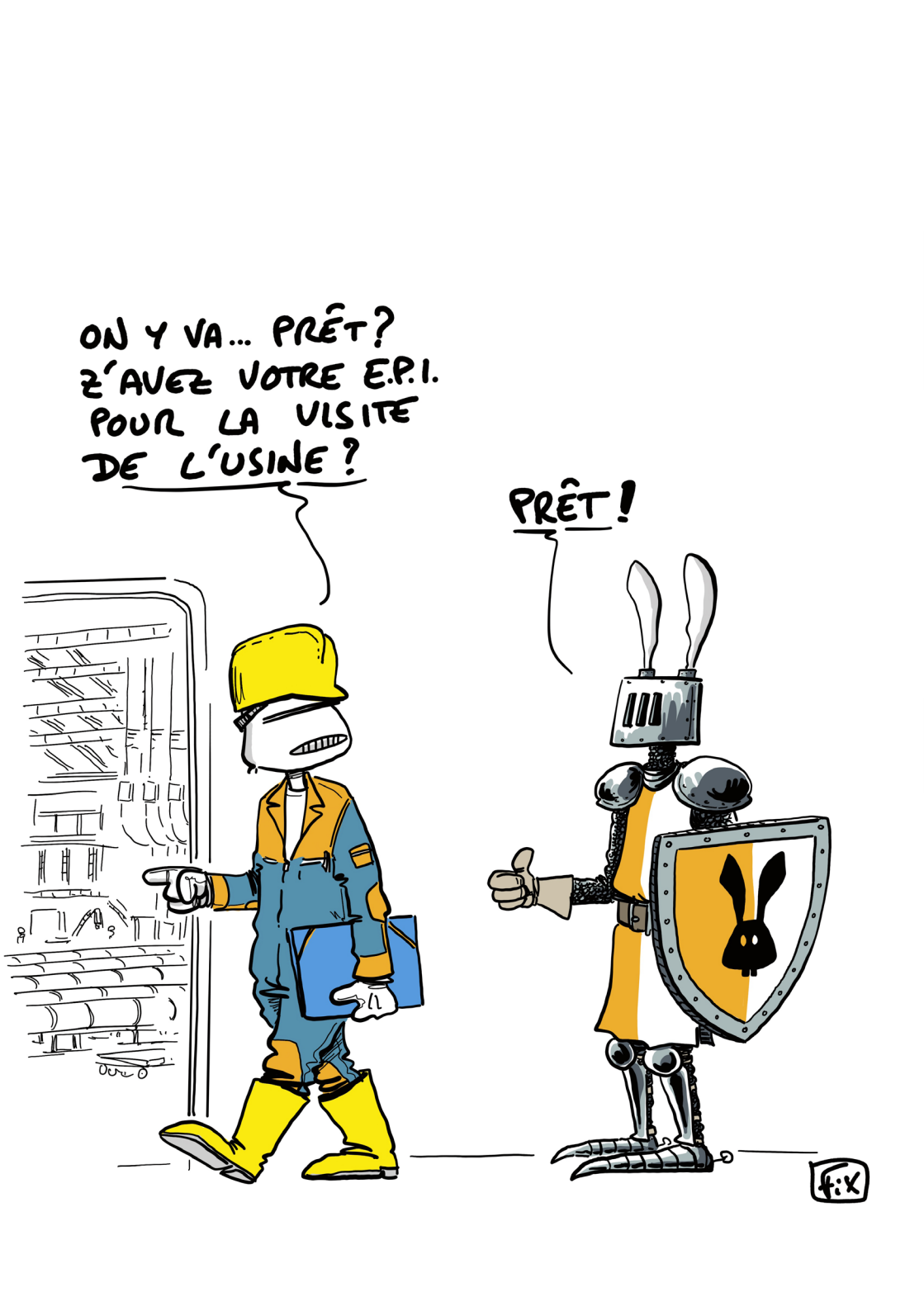
- Dans l'IT, on privilégie le plus souvent la confidentialité (C/I/D);
- Dans l'OT, on privilégie le plus souvent la disponibilité (D/I/C).

DMZ (IT)

En sécurité informatique, une DMZ (Zone démilitarisée ou demilitarized zone en anglais) est un sous-réseau dans lequel sont branchés les équipements qui doivent être accessibles depuis un réseau de moindre confiance (notamment Internet).

L'objectif de la DMZ est d'ajouter un niveau supplémentaire de sécurité, en isolant les équipements exposés dans une zone spécifique, pour ne pas autoriser d'accès direct au réseau plus sensible. Cela permet normalement de limiter la propagation d'une attaque au réseau sensible. Si vous voulez que le réseau OT et le réseau IT d'une usine restent en bons termes, prévoyez une DMZ entre eux.


NOS INTENTIONS SONT PACIFIQUES!
EUH... PAREIL!
ENTREPRISE A
DMZ
ENTREPRISE B
FiX


ON Y VA... PRÊT? Z'AVEZ VOTRE E.P.I. POUR LA VISITE DE L'USINE?
PRÊT!
FIX

E

Entrées / Sorties (E/S) (OT)

Une entrée/sortie, ce n'est pas la porte de l'usine, mais un connecteur sur l'automate, où se branche un bus de terrain et qui peut changer d'état en fonction de l'information reçue d'un capteur ou à envoyer à un actionneur. C'est la frontière entre le monde logique (automate) et le monde physique (capteurs et actionneurs).

Avec les capteurs et les actionneurs en IP, un port Ethernet unique permet la communication avec plusieurs capteurs et actionneurs.

EPI (OT)

Equipement(s) de Protection Individuelle.

En général nécessaire pour approcher des lignes de production, il(s) devrai(en)t faire partie du paquetage de base de toute personne s'intéressant au sujet industriel, y compris le RSSI.

Le costume-cravate n'est pas un EPI et s'accorde assez mal avec les chaussures de sécurité. Et si vous n'aimez pas le jaune fluo, d'autres couleurs existent.

F

Fiabilité (OT)

La fiabilité, c'est l'aptitude d'un dispositif à conserver dans le temps ses caractéristiques annoncées. La fiabilité peut se mesurer par un taux de défaillance, une durée moyenne entre pannes (MTBF, pour mean time between failures) ou encore une probabilité d'accomplir une tâche pendant un temps donné. On peut distinguer la fiabilité prévisionnelle (ce qu'on vous a vendu) et la fiabilité opérationnelle (la vraie vie).

Les API, contrairement aux ordinateurs classiques, sont des équipements très fiables. À rajouter à votre tétraèdre Disponibilité / Intégrité / Confidentialité / Traçabilité.

HAZOP (OT)

H

HAZard OPerability : Méthode d'analyse des risques et de sécurité des fonctionnements en environnement industriel. Son intérêt est l'identification et l'évaluation des situations pouvant représenter un risque pour le personnel ou les équipements, et le déploiement des moyens (procédés, équipements) de prévention adéquats.

Voir également AMDEC. Le choix de AMDEC ou HAZOP relève de la guerre de religion.

N'allez surtout pas vous imaginer que le risque cybersécurité est prévu a priori dans les analyses de risques métier.

H

HSE (OT)

Hygiène Sécurité Environnement.

Le responsable HSE dans l'usine est celui qui a lourde tâche d'éviter les accidents de travail et les non conformités aux règles d'hygiène et environnementales. On peut parler aussi de QHSE si il s'occupe en plus de la Qualité.

Votre pire ennemi si la cybersécurité est une source d'accident de travail ou de perte de qualité. Et votre meilleur ami, si la cybersécurité évite des évènements redoutés.

21

ICS (OT)

Industrial Control System. En français, système de contrôle industriel. L'acronyme SCI n'existe pas. Si vous voulez un acronyme français, utilisez **SNCC** (Système Numérique de Contrôle Commande). Un système de contrôle industriel est un système automatisé qui supervise et pilote un procédé industriel.

Voir également DCS.

IDS/IPS (IT)

Système de Détection d'Intrusion (IDS) ou de Prévention d'Intrusion (IPS).

Si la perspective de pouvoir couper automatiquement un flux supposément malicieux à l'aide d'un IPS semble être formidable, ça peut être catastrophique da ns le cadre d'un processus industriel. Amateurs d'IPS, passez votre chemin ou revenez à un IDS.

IHM (IT/OT)

Interface Homme Machine.
Dans l'IT, il s'agit d'un clavier, d'un écran, d'une souris et du programme qui permet à l'humain d'interagir avec l'ordinateur. Dans l'OT, c'est plus simplement un écran (souvent tactil ou doté de boutons physiques) sur une armoire électrique, permettant d'avoir une vision et/ou un contrôle local d'une partie du procédé industriel.

Latence (OT)

Intervalle de temps entre la fin d'un événement et le début de la réaction à celui-ci. Si la performance d'un système de contrôle industriel se dégrade, la latence augmente.

Concrètement, cela veut dire qu'au lieu de s'arrêter au 2ème étage, l'ascenseur s'arrêtera quelque part entre le 2ème et le 3ème étage.

Ligne de vie (OT)

Une ligne de vie est une forme particulière de Chien de garde qui permet de vérifier en continu que la communication entre deux automates est toujours fonctionnelle.

M

MTBF (OT)

Mean Time Between Failures, temps moyen entre pannes, traduit également en Moyenne des Temps de Bon Fonctionnement pour préserver l'acronyme, bien que le sens ne soit plus le même.

Le temps moyen entre pannes exprime la fiabilité d'un système. Après une analyse de risque (AMDEC ou HAZOP), on tente d'augmenter le MTBF, le plus souvent en doublant les équipements qui ont un MTBF trop faible. Le MTBF d'un système constitué de composants redondants est grossièrement égal au produit du MTBF de chaque composant redondé le constituant.

Mais quand la cause de la panne est une cyberattaque, redonder les composants ne change rien à la fiabilité du système.

Numérique (OT)

N

S'oppose à Analogique. Un ou plusieurs états 0 ou 1, qui pris ensemble permettent de représenter une valeur. Là, normalement, le RSSI IT devrait s'y retrouver.

OPC (OT)

Ce n'est pas une forme de placement financier. OPC est un protocole de communication industriel. De façon basique, OPC permet de centraliser et standardiser, via un serveur, les données venant des automates. Existe en deux versions

- OPC DA (OLE des Process Control), basé sur les technologies de Microsoft, plus ancien.
- OPC UA (Open Platform Communication), standard ouvert, plus récent.

OT (OT)

Operation Technology. En Français, informatique industrielle.
S'oppose traditionnellement à IT, mais vous n'êtes pas obligés de vous opposer aux automaticiens pour autant.

PLC (OT)

Programmable logic controller. Voir API.

PPE (OT)

Personal Protection Equipment. Voir EPI.

Préactionneur (OT)

Interface de puissance d'un système automatisé, situé entre l'interface de sortie de la partie Commande et l'Actionneur de la partie Opérative. Cet élément, souvent électromécanique, peut comporter les diverses protections (surcharges, courts-circuits, sectionnement.) nécessaires à l'Actionneur. C'est dans le préactionneur que transite l'énergie nécessaire au fonctionnement de l'Actionneur.

Vous avez tout compris ?

Procédé industriel (OT)

Un ensemble de méthodes et techniques utilisées pour la réalisation de produits en grande quantité à un coût acceptable. Les détails du procédé industriel sont parfois considérés comme une donnée confidentielle.

Programme CN (OT)

La programmation de Commande Numérique (CN) permet de définir des séquences d'instructions permettant de piloter des machines-outils à commande numérique pour produire un objet, en général à partir de plans réalisés en CAO.

Parfois, ces données comportent un paramétrage tellement spécifique à la machine de destination qu'elles seraient inexploitables sur le même modèle de machine-outil installé dans une autre usine. Vous voyez d'ici comme la sécurisation d'un monde aussi homogène va être simple.

Protocoles réseau (IT/OT)

Il existe des protocoles réseaux spécifiques au contexte industriel. On peut les classer en deux catégories : ceux s'appuyant sur Ethernet et les autres. Pour les premiers, parmi les plus connus, on trouve Modbus-TCP, Profinet, EtherNet/IP, EtherCAT, PowerLink et Sercos, OPC DA et OPC UA.

Les autres reposent sur d'autres médias comme CAN (CANopen, DeviceNet) ou des liaisons séries asynchrones du type RS232 et RS422/485 (Modbus RTU, PROFIBUS, CC-Link). Et pour vous simplifier la vie, pratiquement aucun protocole réseau industriel ne comporte de mécanisme d'authentification. OPC (DA et UA) sont les deux exceptions notoires.

R

Robot (OT)

Equipement multifonctions reprogrammable capable de déplacer des matériaux, des pièces, des outils ou des appareils spéciaux suivant des chemins programmés en vue d'effectuer des opérations de fabrication diversifiées.

L'appareil rangé dans le placard de votre cuisine pourra difficilement rivaliser.

SCADA

Acronyme anglais pour Supervision Contrôle et Acquisition de Données (Supervisory Control and Data Acquisition). Pas d'acronyme français équivalent. Logiciel qui est capable de superviser et de contrôler des automates industriels, afin de piloter un procédé industriel. Il s'exécute sur un ordinateur qu'on appelle également, par extension, SCADA. *Voir également Superviseur.*

Le mot SCADA est fréquemment incorrectement utilisé comme un synonyme pour Système de contrôle industriel, ICS ou SNCC. L'utiliser en ce sens est une excellente façon, pour le RSSI, de se ridiculiser vis à vis des automaticiens.

SIS (IT)

Système Instrumenté de Sécurité. Ensemble d'équipements permettant de garantir qu'un procédé industriel reste dans des limites non dangereuses pour la vie humaine.

Historiquement,les systèmes de sécurité étaient câblés, c'est-àdirequ'ilsfonctionnaient indépendamme nt de tout système programmable. Depuis qu'ils sont programmables, ils sont vulnérables à une cyberattaque. Pensez-y dans vos analyses de risque.

Superviseur (OT)

Ordinateur sur lequel s'exécute le logiciel SCADA.

S

Supervision (OT)

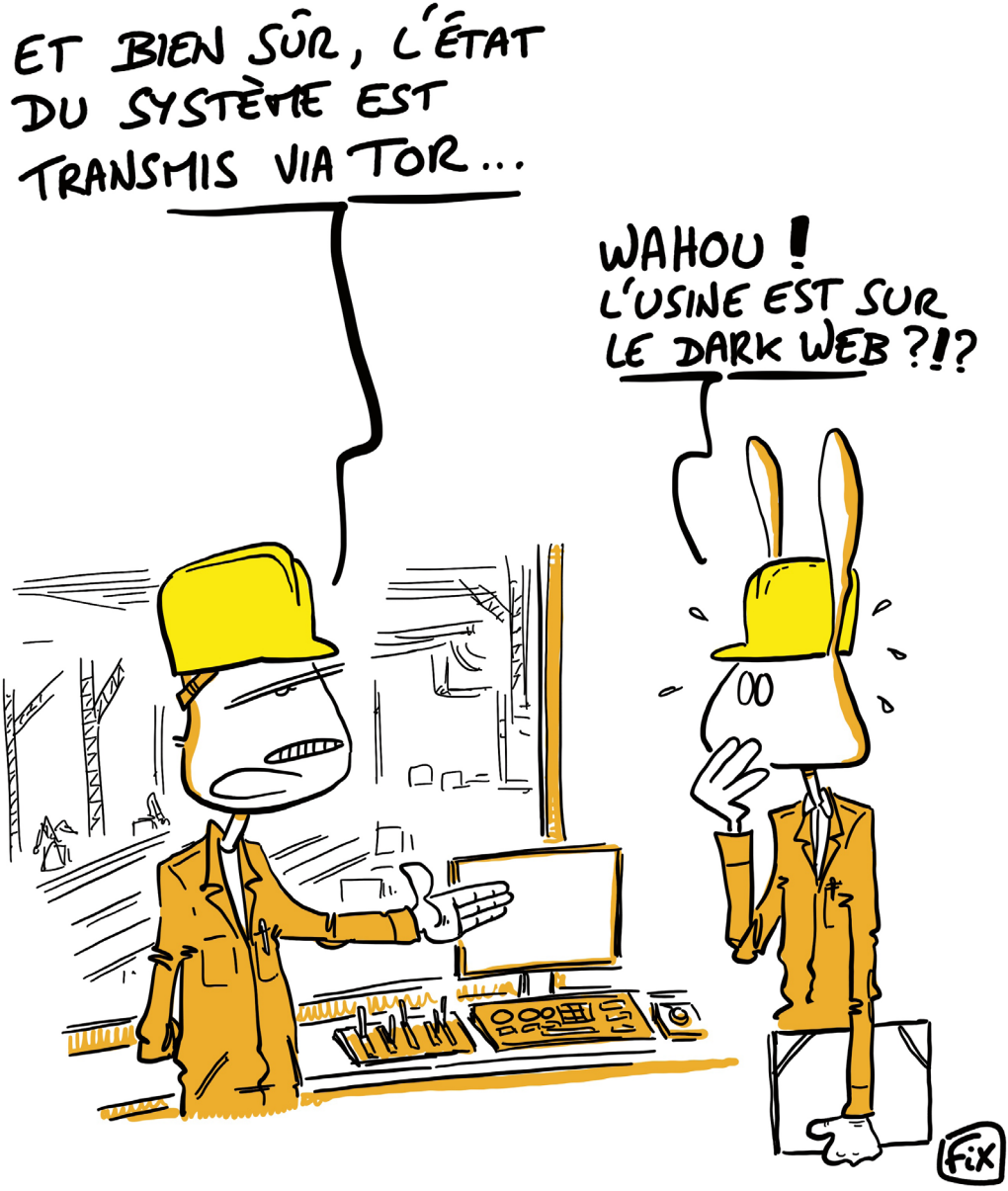
La supervision est - par opposition au contrôle commande - le fait de surveiller le fonctionnement d'un système industriel sans le piloter.

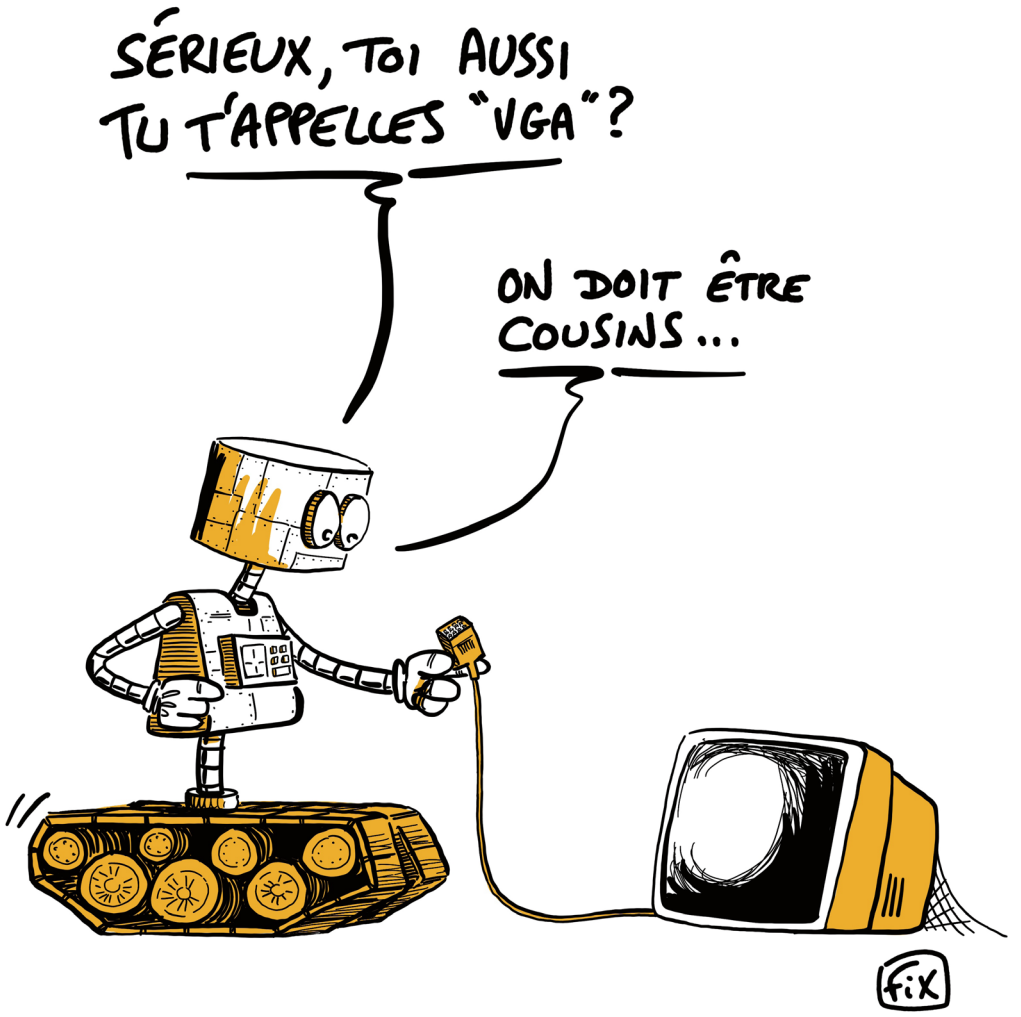
TOR (Tout Ou Rien) vs tor (The Onion Router) (IT/OT)

T

Pour le RSSI, TOR, c'est The Onion Router, le réseau permettant de surfer sur Internet de façon anonyme (et notamment d'accéder au dark web).

Pour l'automaticien, c'est un état Tout ou Rien, c'est à dire un booléen, qui vaut vrai/faux et permet par exemple d'allumer ou éteindre un moteur via un actionneur.


ET BIEN SÛR, L'ÉTAT DU SYSTÈME EST TRANSMIS VIA TOR...
WAHOU ! L'USINE EST SUR LE DARK WEB ?!?
FiX


SÉRIEUX, TOI AUSSI TU T'APPELLES "VGA"?
ON DOIT ÊTRE COUSINS...
fix

VGA (OT)

Non, pour les industriels, ce n'est pas un vieux standard d'affichage. Il s'agit d'un Véhicule à Guidage Automatique (AGV en anglais). Un robot qui déplace de façon autonome des marchandises dans une usine très moderne.

Voteur (OT)

Automate programmable dont le rôle est de choisir entre plusieurs automates quand les ordres qu'ils donnent sont contradictoires afin de poursuivre l'exploitation.

Pas d'abstention possible.

Vraisemblance (OT)

En analyse de risque, la vraisemblance est au risque intentionnel ce que la probabilité est au risque accidentel.. Et la cyberattaque est une cause de panne comme une autre, sauf que la panne simultanée de tous les systèmes en même temps est un scénario réaliste. À méditer entre RSSI et automaticiens.

Remerciements

Merci à toute l'équipe du Lab pour ces après-midi de travail, de rire et d'échanges qui ont permis d'aboutir à ces 3 premiers livrets.

- Nicolas de Pesloüan
- Eric Kawka
- Hervé Delmée
- Benoit Garnier
- Jonathan Boudet
- Patrick Blanluet
- Stephane Tournadre
- Caroline Roche
- Fabrice Bru

Merci à Fix pour avoir su croquer avec humour les travaux du Lab !

Ce guide a été commis par...

Eric Kawka
ERAMET
RSSI Industrie

Fabrice Bru
STIME
Directeur Sécurité des SI

Hervé Helmée
Savencia
RSSI Industrie

Jonathan Boudet
AgroMousquetaires
RSSI

Nicolas de Pesloüan
Veolia
Expert Cybersecurité Industrielle

Benoit Garnier
Mersen
Manager Qualité et Sécurité des Systèmes d'Information Groupe

Patrick Blanluet
Neopost
RSSI Groupe

Caroline Roche
Groupe Pernod Ricard
RSSI Groupe

Stephane Tournadre
Servier
RSSI Groupe

CESIN