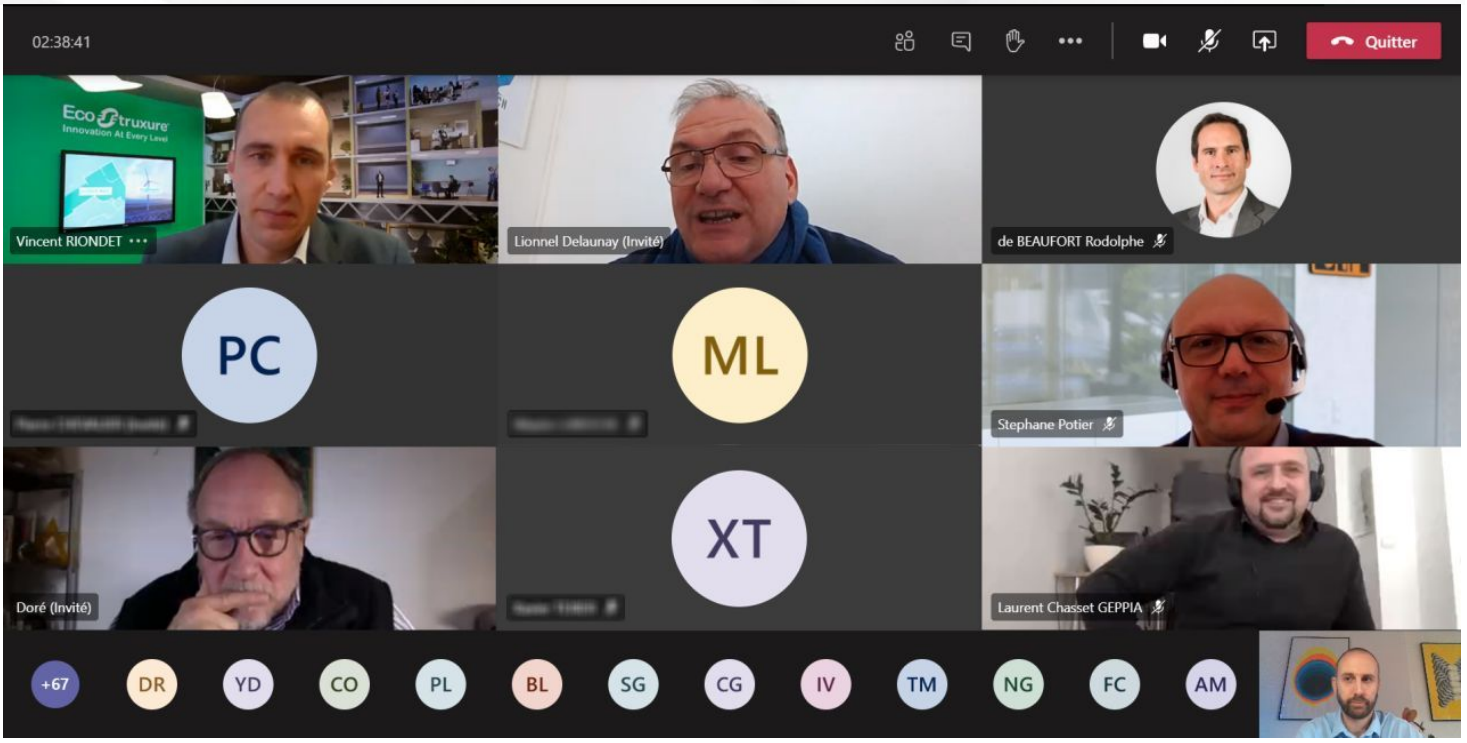
CLUB IDF

Ingénierie Du Futur

GEPPIA

CYBERSÉCURITÉ



Visioconférence du 10 Décembre 2020

Compte-rendu

A l'ordre du jour - Nouvelle formule

Mise en appétit, partage collectif d'informations, actualités

- Santé économique, actualités interclubs

Les enjeux cybersécurité de notre écosystème

- Introduction par Lionnel Delaunay, animateur du Club IDF

GROUPE SAVENCIA : industriel End-User impliqué dans l'Industrie du Futur

- Intervention de Xavier Texier, Responsable Automatismes et OT du groupe Savencia

Advens Vision : 360° de la cybersécurité dans le cadre de la convergence IT-OT

- Intervention de Benjamin Leroux, Directeur Marketing chez Advens

Cybersécurité et OPC-UA :

- Intervention de Stéphane Potier, Responsable marketing OPC-UA France

ROQUETTE : industriel End-User impliqué dans l'Industrie du Futur

- Table ronde animée par Lionnel Delaunay autour du retour d'expérience de la cyber sécurisation des sites de production de la société

GIMELEC : Point technique & approche de normalisation

- Présentation du groupe de travail cybersécurité du GIMELEC par Rodolphe de Beaufort, Directeur Général Adjoint GIMELEC, Animateur du Club Cyber-OT

Téléchargez le dossier des documents présentés : ici

La Team GEPPIA présente

Profitez de cette lecture pour agrandir votre réseau professionnel et suivre les entreprises qui vous intéressent. Cliquez sur les logos Linkedin !

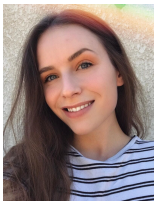
GEPPIA

Jean-Marc Doré
Président
GEPPIA

Laurent Chasset
Marketing-Com°
Développement
GEPPIA

Pierre Chevalier
Stratégie et opérations
GEPPIA

Lionnel Delaunay
Animateur du Club IDF
GEPPIA



Alizée Moreau
Alternante
Marketing Com°
GEPPIA

Intervenants

GROUPE SAVENCIA

Xavier Texier, Responsable Automatismes et OT

GROUPE SAVENCIA : Savencia est un groupe alimentaire international, familial et indépendant, comptant 23 100 collaborateurs dans le monde et commercialisant ses marques dans 120 pays. Le Groupe compte deux entités : Savencia Fromage & Dairy et Savencia Gourmet.

En savoir plus sur GROUPE SAVENCIA

ADVENS

Benjamin Leroux, Directeur Marketing

ADVENS VISION : Pure player français n°1 de la cybersécurité. Advens propose une offre complète de prestations, allant de la stratégie à la gestion opérationnelle de la sécurité, ainsi qu'une suite innovante de services clés en main pour simplifier, rendre agile et accessible à tous la sécurité (Security-as-a-service).

En savoir plus sur ADVENS

OPC UA FRANCE

Stéphane Potier, Responsable marketing B & R

OPC UA FRANCE : Groupe de travail initié par le GIMELEC et l'OPC FOUNDATION. Son objectif : accélérer et promouvoir l'adoption de ce standard de communication entre objets connectés au sein des usines, en particulier au sein des processus de production.

En savoir plus sur OPC FOUNDATION

ROQUETTE

Philippe Pruvost,
Global operations Tech. PMO

Laurent Waymel,
OT Cyber Security Manager

ROQUETTE : Roquette est un leader mondial des ingrédients d'origine végétale, un pionnier des protéines végétales et un fournisseur leader d'excipients pharmaceutiques.

En savoir plus sur ROQUETTE

STORMSHIELD

Vincent Nicaise, Industrial Partnership and Ecosystem Manager

STORMSHIELD : Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Leur objectif : cyber-séréniser leurs clients pour qu'ils puissent se concentrer sur leur cœur de métier, si crucial pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations.

En savoir plus sur STORMSHIELD

SCHNEIDER ELECTRIC

Vincent Riondet, Network Engineering & Cybersecurity

SCHNEIDER ELECTRIC : Schneider Electric fournit des solutions énergétiques et d'automatismes numériques pour l'efficacité énergétique et le développement durable. Leur objectif : rendre les processus et l'énergie sûrs et fiables, efficaces et durables, ouverts et connectés.

En savoir plus sur SCHNEIDER ELECTRIC

GIMELEC

Rodolphe de Beaufort, Directeur Général Adjoint GIMELEC, Animateur du Club Cyber-OT

GIMELEC : Le GIMELEC est le groupement des entreprises de la filière électro-numérique en France. Ses adhérents conçoivent et déploient les technologies et services pour le pilotage optimisé et sécurisé des infrastructures énergétiques et numériques, de l'industrie, des bâtiments et de l'électromobilité. Le GIMELEC valorise leurs technologies et savoir-faire industriels vis-à-vis des marchés et institutions en France et à l'international.

En savoir plus sur GIMELEC

Introduction

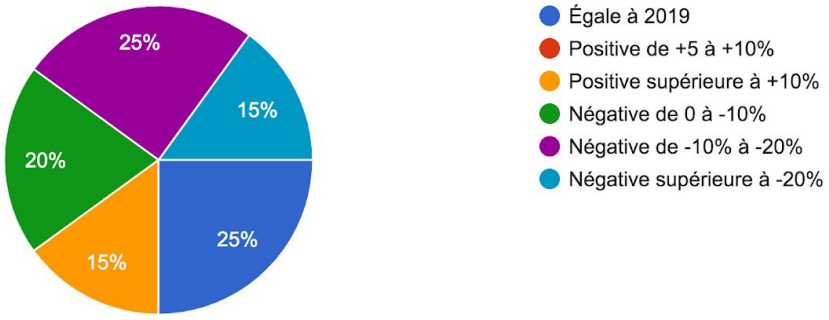
Cette réunion en visioconférence, d'une durée de 2h30, a réuni plus de 80 personnes (sur les 110 personnes inscrites initialement) le jeudi 10 décembre : constructeurs de machines OEM, des partenaires industriels et quelques end-users que nous regrettons de ne pas avoir vu plus nombreux malgré les sollicitations acharnées de la Team Geppia, étant donné la qualité des retours d'expérience de leur confrères (Savencia, Roquette).
Nous avons bien conscience de votre fort intérêt pour la thématique cybersécurité et des besoins grandissants des OEM et des end-users en la matière.

Santé économique

Face au contexte de pandémie mondiale, nous avons profité de nos précédentes réunions pour interroger nos membres sur leur santé économique. Voici les tendances obtenues (20 réponses).

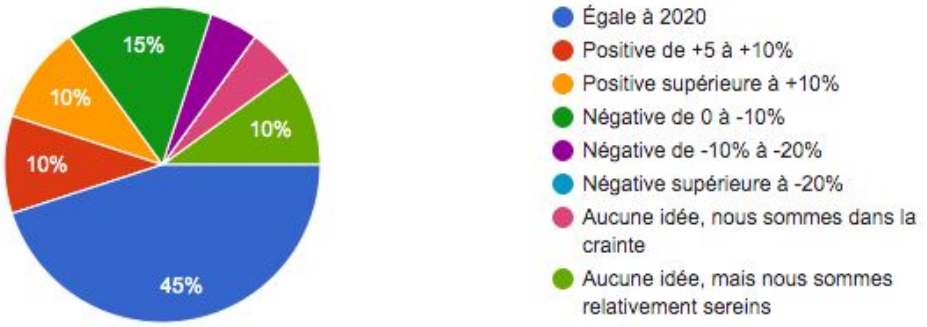
Pour 2020, quelle sera la tendance de votre activité (CA) comparée à 2019 ?

20 réponses



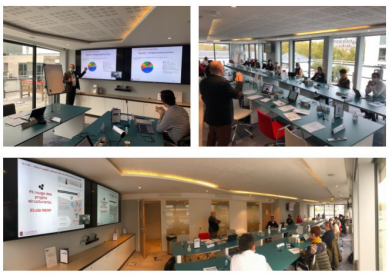
Pour 2021, quelles sont vos (difficiles) projections par rapport à 2020 ?

20 réponses



Le GEPPIA : un réseau & une dynamique de clubs

CLUB IDF
Ingénierie Du Futur



CLUB MARCOM
Marketing & Communication

CLUB ACHATS
Achats industriels

Pour les nouveaux participants, et pour rappel, Jean-Marc Doré a évoqué les trois clubs du GEPPIA : le Club Ingénierie Du Futur, le Club Marcom et le Club des Acheteurs. Avec des réunions trimestrielles et une animation digitale sur notre réseau social inter-entreprises Whaller, l'objectif du GEPPIA est de créer du contact et de l'échange mais également d'accompagner ses membres.

Chaque club a également ses objectifs propres :

- Comprendre les enjeux du 4.0 et innover avec le **Club Ingénierie du Futur**
- Mieux communiquer pour mieux vendre avec le **Club Marcom**
- Bien acheter, échanger entre membres avec **Club des Acheteurs**

Accéder à notre réseau social inter-entreprises Whaller : https://whaller.com/-geppia

Agenda des événements GEPPIA

2021

T1 2021 : Digital event (en préparation)

14/01/2021 : Réunion du club MARCOM

04/02/2021 : Réunion du club ACHATS

11/03/2021 : Réunion du club IDF

25/03/2021 (ou 30/06/2021) : Evénement GEPPIA (en préparation)

20/05/2021 : Réunion du club ACHATS

27/05/2021 : Réunion du club MARCOM

08/06/2021 au 10/06/2021 : Salon CFIA RENNES

24/06/2021 : Réunion du club IDF

01/07/2021 : Réunion du club ACHATS

08/07/2021 : Réunion du club MARCOM

23/09/2021 : Réunion du club MARCOM

28/09/2021 au 30/09/2021 : Salon ALINA BORDEAUX

07/10/2021 : Réunion du club ACHATS

14/10/2021 : Réunion du club IDF

16/11/2021 au 18/11/2021 : Salon Prod&Pack Lyon (ex EUROPACK-EUROMANUT)

* Sous réserve de modifications (mesures sanitaires ou chevauchement de dates événementielles

Introduction à la Cybersécurité

Les enjeux de la cybersécurité de notre écosystème (fournisseurs d'équipements & solutions technos - intégrateurs - end-users).

Introduction par **Lionnel Delaunay**, animateur du Club Ingénierie Du Futur

Pour introduire le thème de la cybersécurité, il est important de rappeler que les attaques existent et toutes les sociétés peuvent être touchées ; les rançons vont de quelques milliers d'euros à des centaines de milliers d'euros.

L'approche de **Savencia** et de **Roquette,** les deux end users qui ont répondu à l'appel pour intervenir sur le sujet de la cybersécurité, sont finalement très proches. Il est nécessaire d'avoir une approche pragmatique et structurée afin d'obtenir des résultats efficaces et pouvant être compris des intégrateurs et fournisseurs.

Ces usecase très bien mis en avant par M. *Xavier Texier* et M. *Laurent Waymel* vont prouver l'accessibilité à la cybersécurité, y compris pour les non-spécialistes.

Nos adhérents OEM constateront que les enjeux d'une stratégie **structurante** dans le domaine de la cybersécurité sera **indispensable** pour réussir à répondre aux demandes de l'usine du futur 4.0

Un industriel end user impliqué dans l'Industrie du Futur

Partage du cahier de spécifications de l'entreprise en termes de cybersécurité.

Intervention de **Xavier Texier**, Responsable Automatismes et OT du **groupe Savencia**, un leader mondial des Fromage & Dairy

Ce que l'on peut retenir des échanges :

Xavier Texier est intervenu afin de présenter le cahier des charges pensé par le Groupe Savencia. Nous avons découvert un formidable exemple de cahier des charges structurant les relations clients-fournisseurs et qui s'impose petit à petit aux fournisseurs de Savencia sans que cela soit vécu comme une contrainte.

Les participants l'ont perçu comme un "livre blanc" de la Cyber à télécharger et partager sans modération !

Téléchargez le cahier des spécifications du Groupe Savencia : ici

Vision 360° de la cybersécurité dans le cadre de la convergence IT-OT

Partage d'un cas d'étude avec des axes de travail pratiques et concrets, à actionner très rapidement.

Intervention de **Benjamin Leroux**, Directeur Marketing chez Advens

Ce que l'on peut retenir des échanges :

La Cybersécurité est un domaine vaste, qui peut sembler complexe. L'industrie du futur conduit à la convergence IT-OT. Quels sont alors les nouveaux risques induits ? Par où commencer lorsque l'on démarre une démarche de sécurité de l'OT ? Comment inscrire ces travaux dans la durée ?

Lors de son intervention, Benjamin Leroux, Directeur Marketing chez Advens a partagé un cas d'étude avec des axes de travail pratiques et concrets.

S'appuyer sur Advens et son expertise pour préparer sa Roadmap Cybersécurité est une évidence suite à la qualité de cette intervention. Comprendre les failles, analyser les faiblesses, appuyer ou cela fait mal pour réussir à se cyberprotéger : tout un programme rendu possible par Advens.

Téléchargez la présentation de Benjamin Leroux : ici

Cybersécurité et OPC-UA

Comment la norme d'interopérabilité OPC UA facilite l'émergence de l'Industrie 4.0 et quels sont ses avantages pour la cybersécurité des architectures IIoT ?

Intervention de **Stéphane Potier**, Responsable marketing OPC-UA France

Ce que l'on peut retenir des échanges :

Stéphane Potier a rappelé les raisons pour lesquelles la norme OPC UA s'imposait dans l'industrie 4.0 : OPC UA permet une interopérabilité verticale avec une seule norme du capteur jusqu'au cloud et assure une interopérabilité horizontale au niveau des lignes de production et de conditionnement.

OPC UA permet ainsi une harmonisation des communications entre les machines, et des machines aux systèmes d'information, rendant ainsi possible la convergence IT/OT.

Stéphane a rappelé qu'OPC UA est "secure by design" car il a été conçu en intégrant les meilleures pratiques de cybersécurité de l'IT et qu'il intègre tous les concepts de sécurité qui permettent de faire face aux menaces qui pèsent sur les systèmes industriels.

Après avoir expliqué les concepts clés de la cybersécurité, Stéphane a présenté les différentes politiques de sécurité intégrées à OPC UA qui lui permettent d'assurer une défense en profondeur des architectures IoT Industriel.

Téléchargez la présentation de Stéphane Potier : ici

Un industriel end user impliqué dans l'Industrie du Futur

Table ronde animée par Lionnel Delaunay autour du **retour d'expérience de la cyber sécurisation des sites de production de la société ROQUETTE**

Interventions de :

- **Laurent Waymel**, OT Cyber Security Manager chez Roquette,
- **Philippe Pruvost**, Global operations Tech.PMO chez Roquette,
- **Vincent Nicaise**, industrial Partnership and Ecosystem Manager chez Stormshield,
- **Vincent Riondet**, network Engineering & Cybersecurity chez Schneider Electric

Ce que l'on peut retenir des échanges :

La quadrature du cercle : Roquette qui nous a expliqué de façon très simple pourquoi et comment il a choisi ses solutions d'architectures cybersécurisées, pourquoi il a retenu l'association Stormshield pour le hardware et Schneider Electric pour l'intégration et le déploiement.

Roquette nous a montré que les choix d'architecture d'automatisme n'excluent pas les vieilles machines. En effet on accepte dans des zones démilitarisées (DMZ) des machines non cybersécurisées en accord avec le principe de demain, on pourra modifier si besoin ces vieilles machines en conformité avec la cybersécurité et un fournisseur non cyber sécurisé pourra être intégré dans cette DMZ.

De plus des solutions comme Bastion nous ont également été présentées par Laurent comme des briques importantes dans cette stratégie de sécurisation.

Une approche intéressante qui ne crée pas de surcoûts pour les OEM.

Merci à nos interlocuteurs pour la qualité des échanges et au dynamisme de Laurent Waymel

---

Téléchargez la présentation de Vincent Nicaise : ici
Téléchargez la présentation de Vincent Riondet : ici

Point technique & approche de normalisation

Présentation du groupe de travail cybersécurité du GIMELEC

Intervention de Rodolphe de Beaufort, Directeur Général Adjoint GIMELEC, Animateur du Club Cyber-OT

Ce que l'on peut retenir des échanges :

Rodolphe nous a montré le rôle stratégique du Gimelec comme leader d'opinion et pour pousser les normes dans ce domaine si important qu'est la cybersécurité.

Le Gimelec est un acteur très proche du Geppia par ses initiatives pleines de bon sens.

Téléchargez la présentation de Rodolphe de Beaufort : ici

Si vous n'avez pas encore reçu d'invitation en provenance de notif@mail.whaller.com (regardez votre courrier indésirable) :

Cliquez sur le lien pour être invité à rejoindre le Club :

https://whaller.com/sphere/4sp1oc

*NB : Vous pouvez vous y inscrire avec votre compte **Linkedin** (pour éviter le énième mot de passe oublié ;-) Cliquez en haut à droite sur s'inscrire, puis sur le logo Linkedin, en bas de la fenêtre pop-up, qui se sera ouverte (sur la version desktop de whaller.com).*

Hotline : (je n'y comprends rien à votre inscription sur whaller…)
> Laurent chasset : 06 77 35 98 78 - laurent.chasset@geppia.com