

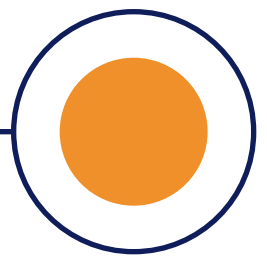
CYBERSÉCURITÉ



**COMMENT GARANTIR
LA CYBERSÉCURITÉ
D'UNE UNITÉ DE
PRODUCTION /
DISTRIBUTION
D'HYDROGÈNE ?**

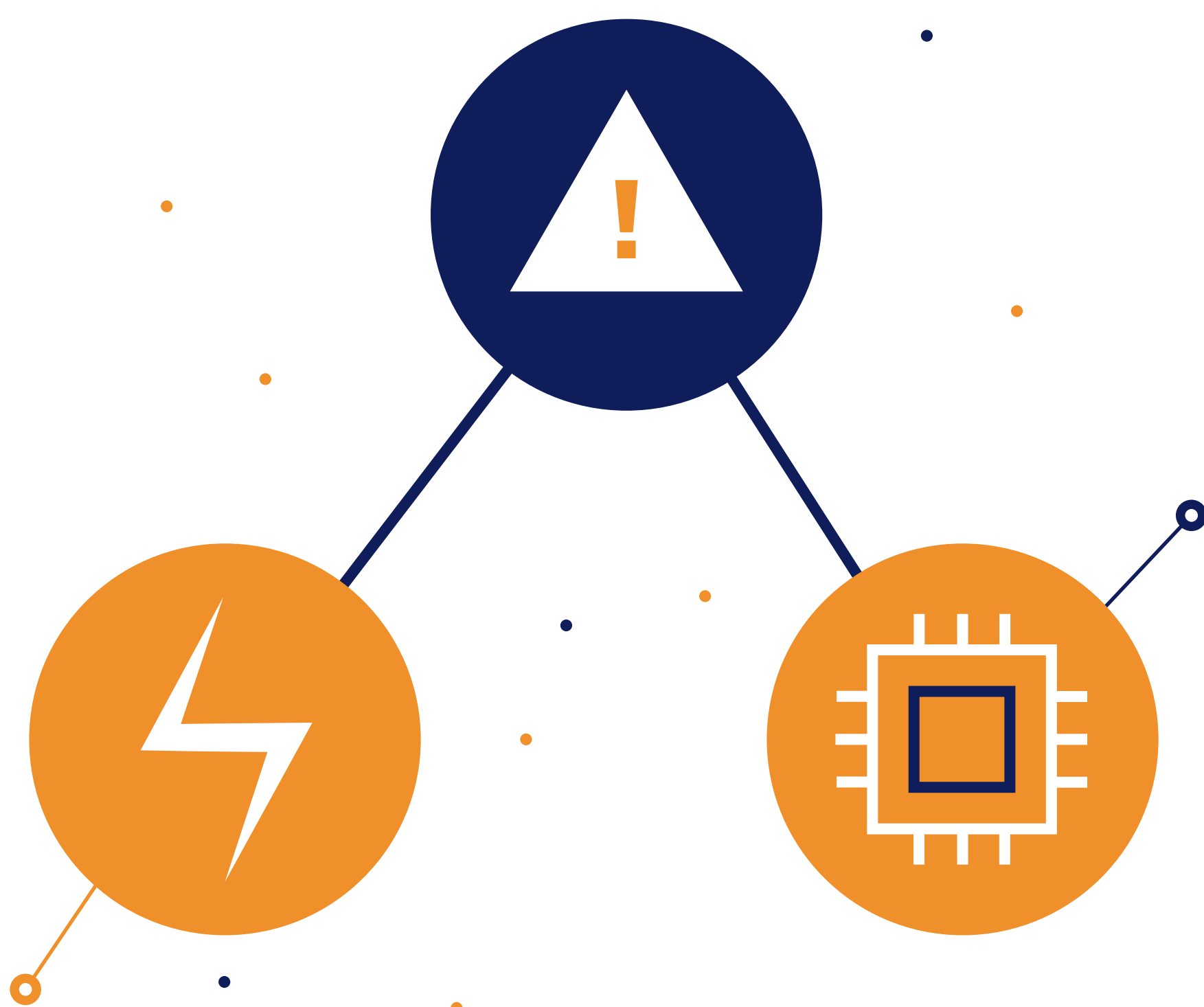
La maîtrise des risques est l'un des enjeux majeurs de la production d'hydrogène. Si l'on pense évidemment aux fuites et aux explosions, **il ne faut pas négliger le risque de malveillance informatique et de cyberattaque** auxquels une installation hydrogène est particulièrement exposée.

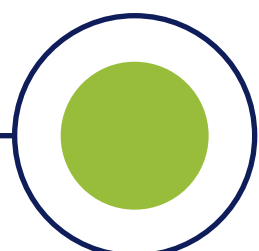




UNE PRODUCTION SENSIBLE

La production d'énergie est aujourd'hui une cible privilégiée pour qui veut paralyser l'activité économique. Une attaque sur des installations hydrogène peut avoir **de lourdes répercussions dans certains secteurs industriels mais aussi pour de nombreux réseaux de transport.**

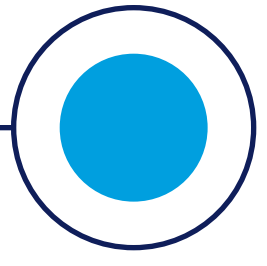




UN PROCESS EXPOSÉ

En amont (sources d'énergies renouvelables multiples) comme en aval (stockage, injection dans le réseau), **le process de production d'hydrogène vert est hyper-connecté. Il est également automatisé et piloté à distance (EMS).** Autant de facteurs qui font de la cybersécurité des installations et des systèmes informatiques un enjeu majeur.

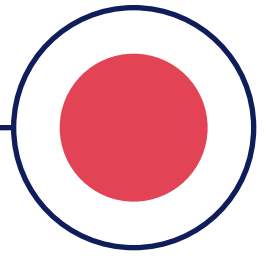




UNE CHAÎNE DE VALEUR CYBERSÉCURITÉ ÉTENDUE

Une défense en profondeur implique donc de mettre en place et de maintenir **un dispositif efficace de cybersécurité pour protéger l'infrastructure informatique et l'infrastructure d'information. Mais aussi, une fois que cette sécurisation est réalisée, d'assurer le fonctionnement des équipements et des applications à tout moment (Maintenance en Conditions Opérationnelles) et la mise à jour du profil de sécurité des systèmes (Maintenance en Conditions de Sécurité).**

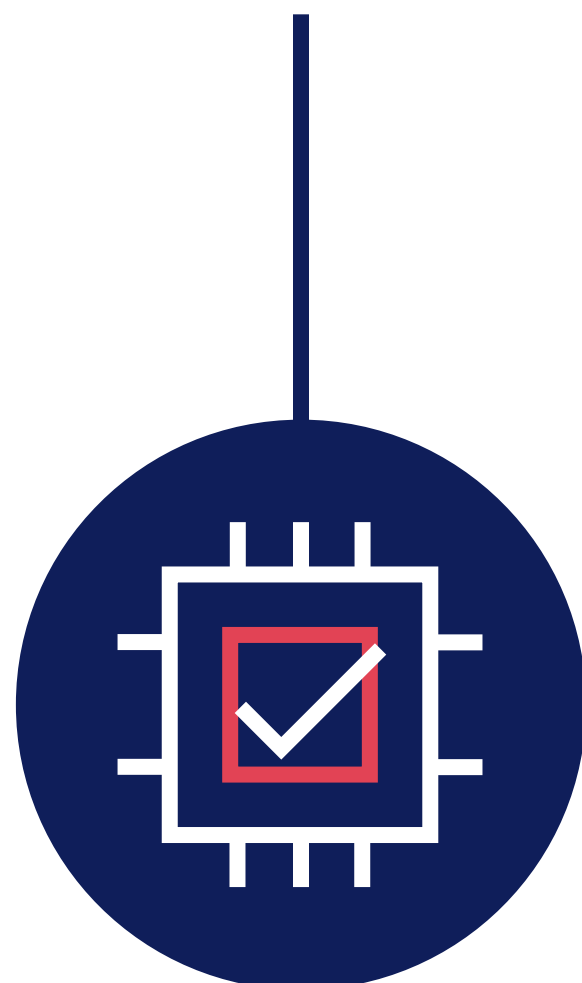




L'APPROCHE INTÉGRALE ONE SPIE

Face à cet écosystème complexe (réseau, informatique industrielle, automatisation), SPIE a développé une approche de la cybersécurité industrielle basée sur

- **la complémentarité entre experts IT (SPIE ICS) et automaticiens (SPIE Industrie).** Une approche misant sur la résolution des contraintes techniques, organisationnelles mais aussi humaines pour créer une culture de la sécurité partagée.





SPIE s'appuie sur une expertise unique en matière d'automatisme et d'informatique industriels et une grande connaissance du secteur de l'énergie. Deux conditions indispensables aujourd'hui pour répondre aux défis posés par la cybersécurité de la production d'hydrogène.



Christophe Winckler

Responsable d'affaires cybersécurité chez SPIE Industrie

