BOOTCAMP INSIGHTS

LES ENSEIGNEMENTS CLÉS DE LA TABLE RONDE :
COMMENT LA DIGITALISATION, LA VALORISATION DES DONNÉES ET LES NOUVEAUX OUTILS AMÉLIORENT LA PLANIFICATION, LA MODÉLISATION ET LA SÉCURITÉ DES RÉSEAUX ?

Cette table ronde, animée par **Jérôme Gaonach (AETS)**, a réuni **Florent Cadoux (Roseau Technologies)**, **Cyril Perret (IED)** et **Ngor Sene (Senelec).**

1. JUMEAUX NUMÉRIQUES : DE LA PROMESSE À LA RÉALITÉ

Les jumeaux numériques deviennent progressivement des outils clés pour **planifier, simuler et fiabiliser** les réseaux électriques. Ils permettent de mieux représenter le fonctionnement réel du réseau, en tenant compte à la fois de sa structure et de son exploitation quotidienne. .

📌 Retours d'expérience

- Grâce aux **compteur intelligents**, decapteurs intelligents et à une meilleure interconnexion des systèmes, les réseaux sont désormais plus **observables.** Les jumeaux numériques offrent la possibilité d'améliorer la cohérence entre les représentations théoriques et l'exploitation réelle.
- Dans ce contexte, la qualité des données constitue un prérequis
- Les modèles ne sont fiables que si les **cas d'usage sont bien définis** : intégration des EnR, réduction de pertes, gestion d'incidents, priorisation de raccordements.
- Le principal défi n'est plus technique, mais **organisationnel** et méthodologique. La réussite d'un jumeau numérique suppose :

→ gouvernance claire (rôles, responsabilités, arbitrages)

→ coordination renforcée entre planification, exploitation et systèmes d'information

→ montée en compétences des équipes pour intégrer ces outils dans les processus métiers existants.

🔑 **Message clef**

On ne rate pas un jumeau numérique à cause du logiciel, mais parce que les objectifs sont insuffisamment définis et que les données sont incomplètes et mal structurées.

2. VALORISATION DES DONNÉES : GUIDER LES INVESTISSEMENTS ET ACCÉLÉRER L'ACCÈS À L'ÉNERGIE

La multiplication des sources de données dans les réseaux électriques – SIG, AMI, télérelève, SCADA, bases patrimoniales ou données ouvertes – permet de transformer les données en **décisions d'investissement plus rapides et plus rationnelles**.

🚀 **Retours d'expérience**

- Les échanges ont mis en évidence une situation largement partagée par les opérateurs. Les données existent, mais leur exploitation reste souvent limitée par
  - Une forte hétérogénéité des sources de données
  - Des niveaux de complétude variables selon les zones
  - Un manque d'alignement des besoins entre les différentes équipes
- Les opérateurs qui réussissent sont ceux qui mettent en place une **gouvernance des données structurée** reposant sur :
  - Des référentiels et standards communs
  - Une meilleure interopérabilité entre les systèmes
  - Des rôles clairement définis
- Une fois organisées, les données permettent des usages à forte valeur ajoutée :
  - Identification des **zones à faible coût de raccordement**,
  - Orientation plus ciblée des extensions et des renforcements,
  - Comparaison des scénarios d'investissement
  - Simulation les besoins à moyen et long terme (**2030–2050),** intégrant les énergies renouvelables, l'évolution de la demande, la flexibilité et les impacts CAPEX/OPEX

🔑 **Message clef**

Les réseaux disposent **déjà** de suffisamment de données pour décider mieux.

L'enjeu n'est plus de multiplier les outils ou les sources, mais de structurer les données existantes et de **les exploiter efficacement.**

3. CYBERSÉCURITÉ & INTEROPÉRABILITÉ : UN ÉQUILIBRE EXIGEANT

La digitalisation des réseaux électriques repose de plus en plus sur l'interconnexion des systèmes (SCADA, AMI, SIG, applications web et interfacesAPI). Cette ouverture indispensable pour améliorer l'efficacité opérationnelle des opérateurs augmente mécaniquement la **surface d'attaque**. Dans ce contexte la cybersécurité ne peut plus être traitée comme un sujet annexe mais doit être pensée **dès la conception** des systèmes.

🛡️ Retours d'expérience

- Les échanges ont souligné un constat partagé. L'ouverture des systèmes est désormais inévitable, mais elle doit être maîtrisée dès la conception. Les principes mis en avant reposent sur une approche security-by-design, incluant notamment :
  - Le chiffrement systématique des échanges,
  - La segmentation des réseaux,
  - L'application du principe du moindre privilège
  - Des tests réguliers (audits, tests d'intrusion, revues de configuration).
- La **supervision continue** apparait comme un levier essentiel. La mise en place de journaux, d'outils de détection (SIEM) et de capacité d'identification rapide des incidents devient une nécessité
- L'usage croissant de **l'IA** qui permet des attaques plus ciblées. Ceci renforce la nécessité de dispositifs de confinement, de plans de réponse aux incidents et de stratégie de réduction d'impact.
- **L'hébergement** reste un point structurant :
  - Les solutions *cloud* offrent agilité, évolutivité et mise à jour rapide, mais soulèvent des enjeux de **souveraineté** (serveurs US).
  - Les solutions *On-premise* peuvent apporter un meilleur contrôle, mais peuvent s'accompagner d'un coût plus élevé et d'une moindre flexibilité

🔑 Message clef

À mesure que les systèmes s'ouvrent et s'interconnectent, la cybersécurité devient un pré-requis opérationnel.La seule approche viable repose sur une cybersécurité pensée dès la conception, une supervision continue et des choix d'architecture cohérents avec les enjeux de souveraineté et de continuité de service.

CONCLUSION GÉNÉRALE

Les échanges ont mis en évidence que la transformation numérique des réseaux électriques ne se limite pas au déploiement de nouveaux outils. Elle repose sur une approche structurée, combinant vision stratégique, valorisation des ressources existantes et maîtrise des risques associés à l'ouverture des systèmes.

1. **La vision avant la solution** : Il n'existe pas de digitalisation efficace sans besoins clairement exprimés et sans processus opérationnels définis. La réussite des projets numériques dépend avant tout de la capacité des opérateurs à formaliser leurs objectifs, à aligner les acteurs internes et à inscrire les outils dans les pratiques métiers existantes. La vision stratégique doit précéder le choix des solutions technologiques.
2. **La donnée comme actif stratégique** : La donnée devient un levier central pour réduire les incertitudes et guider les décisions. Lorsqu'elle est organisée et exploitée de manière cohérente, elle permet d'objectiver les choix d'investissement, d'améliorer la planification des réseaux et de contribuer plus efficacement à l'accès à l'énergie, tout en maîtrisant les coûts et les risques.
3. **Une cybersécurité intégrée de bout en bout** : L'interconnexion croissante des systèmes rend la cybersécurité non optionnelle. Elle doit être intégrée dès la conception des architectures, depuis les capteurs et équipements de terrain jusqu'aux systèmes centraux et aux solutions cloud. La résilience des réseaux et la continuité de service en dépendent désormais directement.

Co-funded by the European Union
Global Gateway
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT
D4D HUB
DIGITAL & GREEN INNOVATION ACTION
Digital Energy