

# Défis collectifs industriels

Projet CyberExcellence  
<https://cyberwal.be/cyberexcellence/>  
Jeudi 06/04/2023

# Liste des WP CyberExcellence :

## WP

WP1 : Rendre les systèmes résilients aux cyberattaques : phase de conception.

WP2 : Détection, Réponse, Réaction : Phase Dynamique

WP3 : RGPD et Open data : sécurité à la conception

WP4 : La protection et le partage des données au cœur des préoccupations

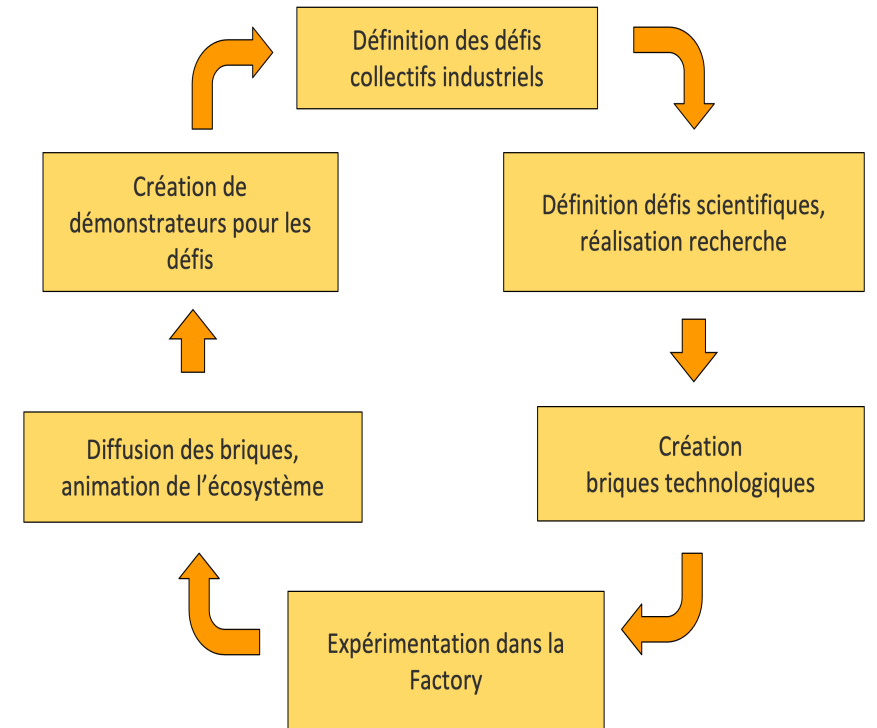
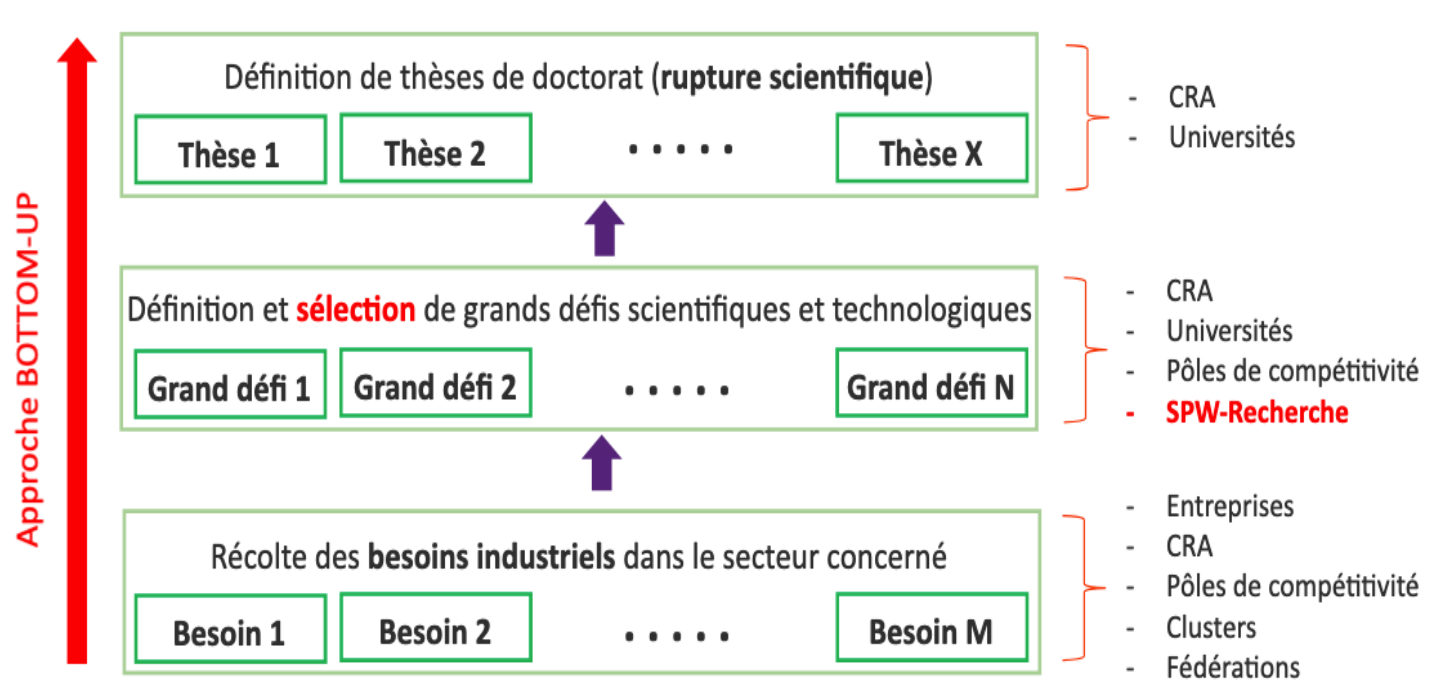
WP5 : Laboratoires d'expérimentation, de validation, et d'entraînement

WP6 : Factory et **Grands Défis**

# WP 6 : Défis Collectifs Industriels

## • Défi Collectif Industriel

- Récolte des besoins industriels dans le secteur concerné
- Identification des défis Collectif Industrie



# Consultation régulière des entreprises

- Première analyse de besoins
  - Démarré avant dépôt du projet
- Définition de défi collectif industriel
  - Défis publiés et extension du nombre d'entreprises intéressées
  - Mise en place de groupes de travail pour affiner les besoins et orienter la recherche
- Résultats de la consultation sur les défis :
  - Mise à jour des défis industriels sur base de la consultation
  - Défis x WP/chercheurs : définition de problèmes de recherche

The screenshot shows the Cyberwal website interface. At the top, there is a navigation menu with links for ACCUEIL, LES ENJEUX, FORMATION, INNOVATION, RECHERCHE, and PARTENAIRES. Below the navigation, the page title is 'CyberExcellence: Grands Défis'. The main content area contains an introduction paragraph, a list of three objectives, and a list of current challenges. At the bottom, there are three sections for user interaction: a section for being informed of results, a section for participating in a working group, and a section for submitting a study case. Each section has radio buttons for 'Oui' and 'Non'. There are two large text input fields for comments and a blue button labeled 'ENVOYEZ VOTRE AVIS'.

digital wallonia cyberwal Cyberwal ACCUEIL LES ENJEUX FORMATION INNOVATION RECHERCHE PARTENAIRES À PROPOS DE Cyber Security in Wallonia

Accueil » CyberExcellence: Grands Défis

## CyberExcellence: Grands Défis

La cybersécurité est et demeurera un enjeu majeur. Toutefois, l'écosystème wallon n'est pas encore suffisamment structuré et les entreprises, privées ou publiques, ne sont pas assez sensibilisées aux risques, aux conséquences et par conséquent, aux procédures à mettre en place.

En amont du projet, des entreprises actives dans le domaine ont été consultées avec l'objectif de détecter des premiers besoins. Ceux-ci sont la plupart du temps des demandes de solutions applicatives répondant à des besoins particuliers et partagés par plusieurs acteurs. Contrairement à d'autres secteurs d'application, un travail préalable est nécessaire pour

1. traduire les besoins en « Grands Défis » collectifs,
2. s'assurer que ces Grand Défis correspondent à une recherche de pointe à bas TRL d'aujourd'hui et de demain,
3. vérifier que les challenges scientifiques qui en découlent sont valorisables à court-terme par le tissu économique.

Les Grands Défis actuels, de nouveaux défis étant identifiés pendant toute la durée du projet, sont les suivants :

- Automatisation de la vérification cybersécurité de systèmes cyber physiques
- Gestion des risques pour tests de pénétration
- Cyber-sécurisation « by design » de systèmes cyber-physiques
- Configuration sécurisée d'infrastructure de communication IoT « by design »

Je suis intéressé d'être informé des résultats des recherches sur ce défi

Oui  Non

Je suis intéressé de participer à un groupe de travail résultats des recherches sur ce défi (réunion/audio conférence 2 fois par an)

Oui  Non

Je souhaite soumettre une étude de cas pour ce défi :

Commentaires sur ce défi :

ENVOYEZ VOTRE AVIS

# Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques

- Personne de contact : Philippe Massonet
- Problème industriel :
  - Cyber Physical System = système intelligent incorporant des réseaux de composants logiciels et physiques qui interagissent entre eux
  - Vérification par les tests fonctionnels (architecture de cybersécurité) et tests de pénétration
  - Phase de création des tests requiert des experts en cybersécurité
  - Nécessité d'automatiser la phase de création, car beaucoup d'outils à utiliser pour les tests de pénétration

# Défi 02 : Gestion des risques pour tests de pénétration

- Personne de contact : Christophe Ponsard (CETIC)
  - Problème industriel :
    - Systèmes industriels de plus en plus exposés aux attaques cyber (transformation numérique vs systèmes SCADA « legacy »)
    - Aspect également de plus en plus régulé dans les domaines essentiels (NIS) avec des référentiels/standards spécifiques IT/OT
    - Activités de test de pénétration très coûteuse en ressources et potentiellement inefficace si pas couplée à une démarche d'analyse des risques
- => nécessité d'automatiser et de conduire les tests selon le risque encouru**

# Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques

Personne de contact : Sébastien Dupont (CETIC)

Problème industriel :

- Cyber Physical System = système intelligent incorporant des réseaux de composants logiciels et physiques qui interagissent entre eux
- Domaines privilégiés : Industrie 4.0 & spatial
- Besoin d'une plus grande puissance de calcul déportée et accroissement des communications nécessaires entre ces composants ou avec un système central
- Approche DevSecOps

# Défi 07 : Configuration sécurisée d'infrastructure de communication IoT « by design »

- Personne de contact : Nicolas Point (MULTITEL)
- Problème industriel :
  - Sécurisation des infrastructures de communication (principalement mobiles)
  - Communication des équipements de type IoT dont l'utilisation ne fait que croître
    - Communications dans la zone OT d'une entreprise
    - Communications en espace "public" : Smartcities, Intelligent Transport Systems...
  - En conjonction avec d'autres défis (réseaux énergétiques, CPS...)



# Défi 10 : Sécurisation de la Digitalisation des Réseaux Énergétiques

- Personne de contact : Benoit Donnet (Uliège)
- Problème industriel :
  - Digitalisation des systèmes de distribution énergétique
    - Environnement distribué
    - Environnement sensible
  - Comment détecter au plus vite une attaque et assurer la continuité du business ?

# Nouveaux Défis

- De nouveaux défis peuvent être définis en cours de projet
  - Initiaux mais pas encore concrétisés : IA/Cyber (cf. TRAIL/ARIAC)...
  - Prévu : Aspects Légaux/RGPD/Normes
  - Autres problématiques possibles en fonction des discussion entre le consortium et les entreprises