Date 08/11/2022

Défis Collectifs Industriels

Journée des chercheurs 8/11

Philippe Massonet
Coordinateur Scientifique CETIC
Philippe.massonet@cetic.be

Responsables de défis:
Philippe Massonet (philippe.massonet@cetic.be),
Christophe Ponsard (christophe.ponsard@cetic.be),
Sébastien Dupont (sebastien.dupont@cetic.be),
Nicolas Point (point@multitel.be),
Benoît Donnet (benoit.donnet@uliege.be)

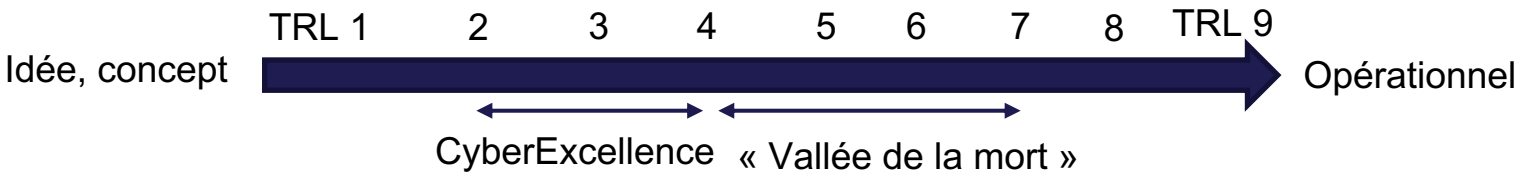
https://cyberwal.be
https://cyberexcellence.be

Défi Collectif Industriel, Identification

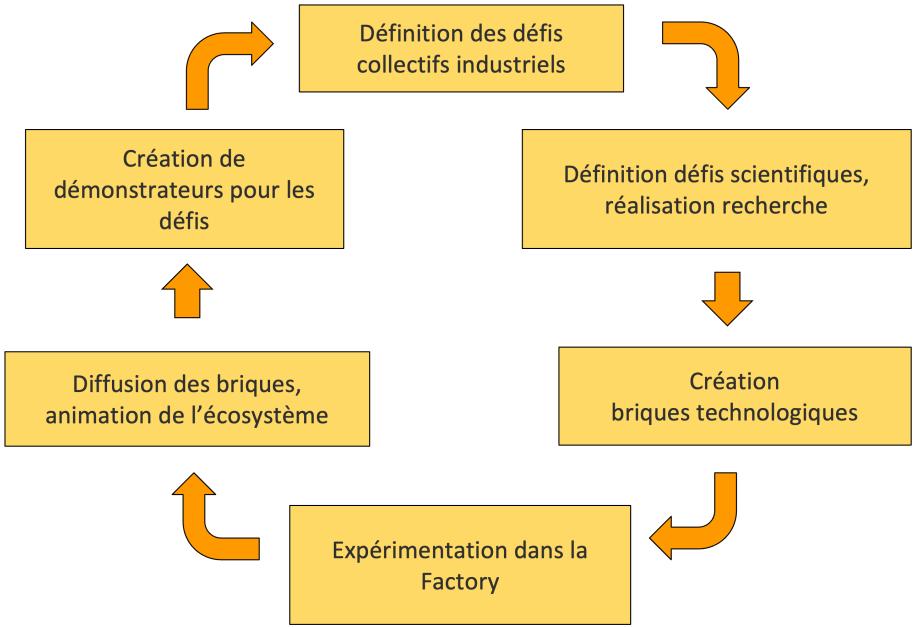
- Défi R&D industriel collectif = problème rencontré par un grand nombre d'entreprises d'un même secteur ou de secteurs différents
    - Les défis correspondent à des problèmes de recherche qui sont ancrés dans les besoins du tissu socio-économique wallon.
    - Identifie un problème fondamental à résoudre pour innover dans les DIS.
- Identification
    - Traduire les besoins en défis collectifs. Des études de cas sont documentées de manière régulière avec les entreprises pour identifier l'évolution des besoins et identifier des défis initiaux et nouveaux défis
    - S'assurer qu'ils répondent à une recherche de pointe à bas TRL
    - Vérifier que les challenges scientifiques qui en découlent sont valorisables à court-terme par le tissu économique.

Défi, Problème de recherche, Factory et Valorisation

- **Défis**: canaliser les travaux sur des enjeux essentiels identifiés dans les DIS pour la Région Wallonne.
- **Problèmes de recherche**: pour chacun des défis, différentes approches de recherche seront identifiées et déboucheront sur des travaux de recherche qui explorent les voies technologiques les plus prometteuses.
- **Briques technologiques** et **démonstrateurs**: les résultats de la recherche seront concrétisés par des briques technologiques de TRL2-4 qui seront expérimentées dans la Factory afin de vérifier si la brique technologique résout le défi technologique.
- **Implémentation successive** de défis collectifs industriels de la CyberWal-Factory de faire **monter en maturité** les recherches algorithmiques effectuées dans les WP1-5. Elle permet aussi de



Méthodologie de travail par Défi



Phase	Chercheurs	Entreprises
identification des besoins (études de cas)	demande études de cas	proposition d'études de cas
identification du défi	définition	
identification des problèmes de recherche	définition	commentaires
réalisation de la recherche	réalisation	commentaires
définition des démonstrateurs	déploiement dans la factory	accès, commentaires

Organisation des défis

- Organisation des défis
  - 15 défis identifiés dans la proposition
  - Actuellement, on travaille sur 5 défis
  - Nouveaux défis générés par une démarche d'open innovation sur 3 cycles complets de 2 années
- Matrice croisée Défis-WP/tâches

Grand défi	WP1	WP2	WP3	WP4	WP5
Défi 01: Automatisation de la vérification cyber de CPS (Contact : Philippe Massonet)					
	T1.2 Tests			Eventuellement T4.4 (attaques contre les implémentations matérielles)	Tâche 1 : Génération automatique de scénarios d'attaque ou de défense pour l'entraînement et la recherche.
					Tâche 2 : Synthèse de séquence d'attaques à partir de base de données de vulnérabilités
Défi 02: Gestion des risques pour tests d'intrusion (Contact : Christophe Ponsard)					
	WP1: Génération automatique de scénarios d'attaque ou de défense pour l'entraînement et la recherche		Risques liés à la confidentialité des données et RGPD: exigences (T3.1), design (T3.2) et risques résiduels liés à l'anonymisation / pseudonimisation (T3.3)	WP4: Conception de processus d'ingénierie DevSecOps: modélisation, performance, en particulier collecte d'indicateurs d'efficacité des mesures de sécurité	
Défi 04: Cyber-sécurisation by design systèmes industrie4.0 et spatiaux (Contact : Sébastien Dupont)					
		WP2 : Détection, Réponse, Réaction: Phase Dynamique	WP3	Tâche 4.2 : Déploiements sûrs à travers le continuum des clouds et edge souverains	WP5 : CyberLabs (hybride)
Défi 07: Configuration de transmission réseaux de données (Contact : Nicolas Point)					
	WP1: Rendre les systèmes résilients aux cyberattaques: phase de conception Tâche 1.1 sur la certification au moyen de modèles mathématiques.			Tâche 4.3 : Vers un chiffrement évolué/robuste et adaptation des protocoles cryptographiques Tâche 4.2 : Déploiements sûrs à travers le continuum des clouds et edge souverains (à confirmer)	

https://cyberwal.be/cyberexcellence-grands-defis/

Défis Actuels et Responsables

Défi	Responsable
Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques	Philippe Massonet
Défi 02 : Gestion des risques pour tests de pénétration	Christophe Ponsard
Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques	Sébastien Dupont
Défi 07/11 :Configuration sécurisée d'infrastructure de communication IoT « by design »	Nicolas Point
Défi 10 : Sécurisation de la Digitalisation des Réseaux Énergétiques	Benoît Donnet

Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques 2/3

- Challenges de recherche:
  - Génération automatique des tests de cybersécurité fonctionnels (architecture de sécurité), utilisation de différentes techniques de génération (à comparer) pour les tests de pénétration:
    - Techniques de fuzzing
    - Génération de tests par mutation génétique
    - Génération de tests à partir de modèles
    - ...
  - Automatisation partielle sous forme d'assistance du processus de création et de la définition des tests de pénétration.
  - « Risk-based testing » pour trouver un meilleur ROI (vulnérabilités/attaques trouvées/budget de test)

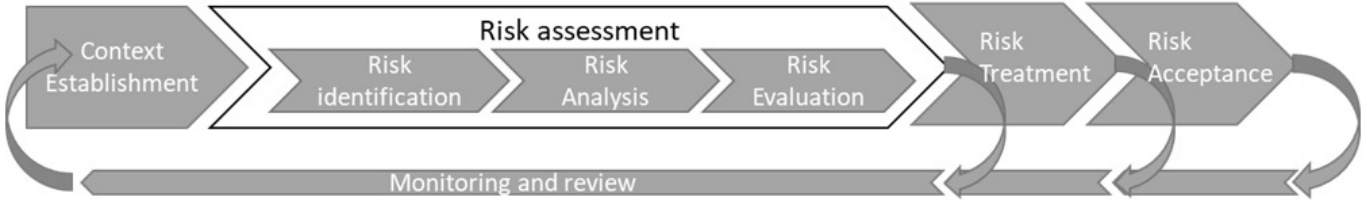
Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques 3/3

- Impact
  - Amélioration de la qualité des tests de cybersécurité -> meilleure protection des infrastructures et applications, et réduction du risque
  - Amélioration du niveau d'automatisation des tests de cybersécurité -> plus d 'entreprises réaliserons des tests de cybersécurité.
    - Tests fonctionnels
    - Tests de pénétration
  - A terme transfert d'une partie des résultats de recherche dans la pratique + « best practice »
- Equipes universitaires/CRA
  - Prof Xavier Devroey (Unamur)
  - Prof Axel Legay (UCLouvain)
  - Guillaume Ginis, Sébastien Dupont, Valery Ramon, Philippe Massonet, … (CETIC)
  - Nicolas Point (Multitel)

Défi 02 : Gestion des risques pour tests de pénétration 1/2

- Personne de contact : Christophe Ponsard (CETIC)
- Problème industriel :
  - Systèmes industriels de plus en plus exposés aux attaques cyber (transfo 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 02 : Gestion des risques pour tests de pénétration 2/2

- Challenges de recherche :
  - Génération automatique de scénarios d'attaque ou de défense pour l'entraînement et la recherche
  - Conception de processus d'ingénierie DevSecOps : modélisation, performance, en particulier collecte d'indicateurs d'efficacité des mesures de sécurité, estimation/apprentissage de vraisemblance
- Impact :
  - meilleure efficacité des processus de tests de pénétration (automation)
  - meilleure couverture des risques cybersécurité
  - meilleur réutilisabilité et alignement avec des référentiels industriels certifiants/NIS
- Equipes universitaires/CRA
  - Christophe Ponsard, Philippe Massonet, Valery Ramon, Denis Darquenne (CETIC)
  - Prof. Axel Legay (UCLouvain)

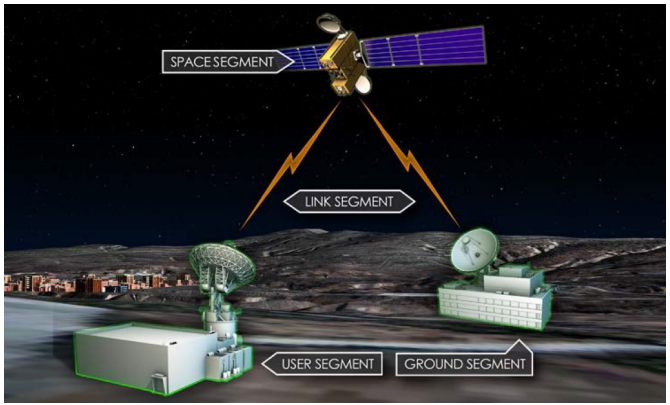
Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques 1/3

Personne de contact : Sébastien Dupont (CETIC)

Problème industriel :

- Domaines : Industrie 4.0 & spatial
- Cyber Physical System = système intelligent incorporant des réseaux de composants logiciels et physiques qui interagissent entre eux
- besoin d'une plus grande puissance de calcul déportée
- accroissement des communications nécessaires entre ces composants ou avec une partie centrale
- Nécessite une haute tolérance aux pannes, facilité de mise à jour

Security in Industry 4.0 - source : Syna.ch

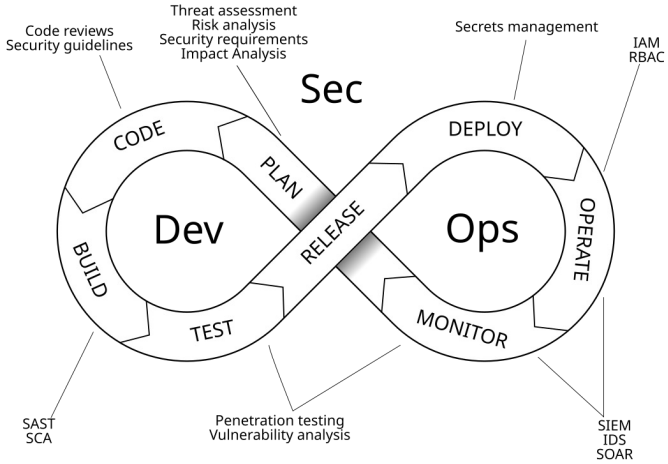


Bailey, B., et al. « Defending spacecraft in the cyber domain. » Aerospace Corp. TR OTR202000016, El Segundo, CA (2019).

Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques 2/3

Challenges de recherche:

- Etudier l'application de méthodes et outils en tenant compte des spécificités de ces domaines
- Démontrer le succès de l'approche DevSecOps
- Sécurité « By Design »
  - sécuriser en profondeur - modèle « zero trust »
  - minimiser la surface d'attaque
  - éviter la sécurité par l'obscurité
  - rester simple
  - CNSSI 1200, CCSDS 352.0-B ou 357.0-B, NIST, ISA/IEC - 62443 ou FDAM



Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques 3/3

Impact

- Détecter les vulnérabilités au plus tôt

  —> minimiser leur impact

  —> réduire le risque

- Convergence entre l'IT et l'OT

  —> unifier le contrôle et la surveillance

  —> faciliter la gestion de la sécurité

Equipes universitaires/CRA

- Sébastien Dupont, Guillaume Ginis, Valery Ramon, Philippe Massonet (CETIC)
- Prof. Jean-Noël Colin (UNamur), Prof. Benoît Donnet (ULiege), Prof. Jean-Michel Dricot (ULB), Prof. Axel Legay (UCLouvain)

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" : Smart cities, Intelligent Transport Systems...
  - En conjonction avec d'autres défis (réseaux énergétiques, CPS...)
- Challenges de recherche
  - Étude et implémentation de tous les éléments assurant un niveau de sécurité très élevé de la transmission des données, du capteur au serveur final de stockage (éventuellement dans le cloud)
  - Développement de composants cryptographiques, d'infrastructures et/ou de protocoles adaptés ou développés spécifiquement

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

- Impact
  - Amélioration de la cybersécurité des infrastructures IoT (dès l'installation)
  - Développement de produits concurrentiels (de plus en plus de demandes des clients)
  - Alignement (ou anticipation) avec les référentiels industriels (NIS...)
- Equipes universitaires/CRA (nom des personnes)
  - Prof. Axel Legay (UCL)
  - Prof. Benoit Donnet (ULiège)
  - Christophe Ponsard (CETIC)

Défi 10 : Sécurisation de la Digitalisation des Réseaux Énergétiques

- Personne de contact: Benoit Donnet
- 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 ?
- Challenges de recherche
    - représentation de du graphe d'inter-dépendance des micro-services
    - observabilité du graphe
    - méthode de détection distribuée
    - unikernels pour limiter la durée de vie des exploits
    - redirection du trafic

Défi 10 : Sécurisation de la Digitalisation des Réseaux Énergétiques

- Impact
  - Meilleure résilience des réseaux énergétiques
  - Continuité du business
- Equipes universitaires/CRA (nom des personnes)
  - Prof. Benoit Donnet (ULiège)
  - Prof. Laurent Mathy (ULiège)

Chercheurs et Défis

- Chaque chercheur engagé par le projet CyberExcellence s'engage dans ses activités de recherche dans une démarche collaborative avec les partenaires impliqués dans son workpackage d'activité et s'engage à allouer au minimum 15% de son temps de travail à participer aux défis du CyberWal-Factory (voir WP6) intégrée dans le volet recherche.

- On doit identifier quel chercheur travaille sur quel défi (problème de recherche, résultat attendu (brique technologique), démonstrateur

- Venez discuter avec les responsables de défis (stand défis)

Défi	Responsable
Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques	Philippe Massonet
Défi 02 : Gestion des risques pour tests de pénétration	Christophe Ponsard
Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques	Sébastien Dupont
Défi 07/11 :Configuration sécurisée d'infrastructure de communication IoT « by design »	Nicolas Point
Défi 10 : Sécurisation de la Digitalisation des Réseaux Énergétiques	Benoît Donnet

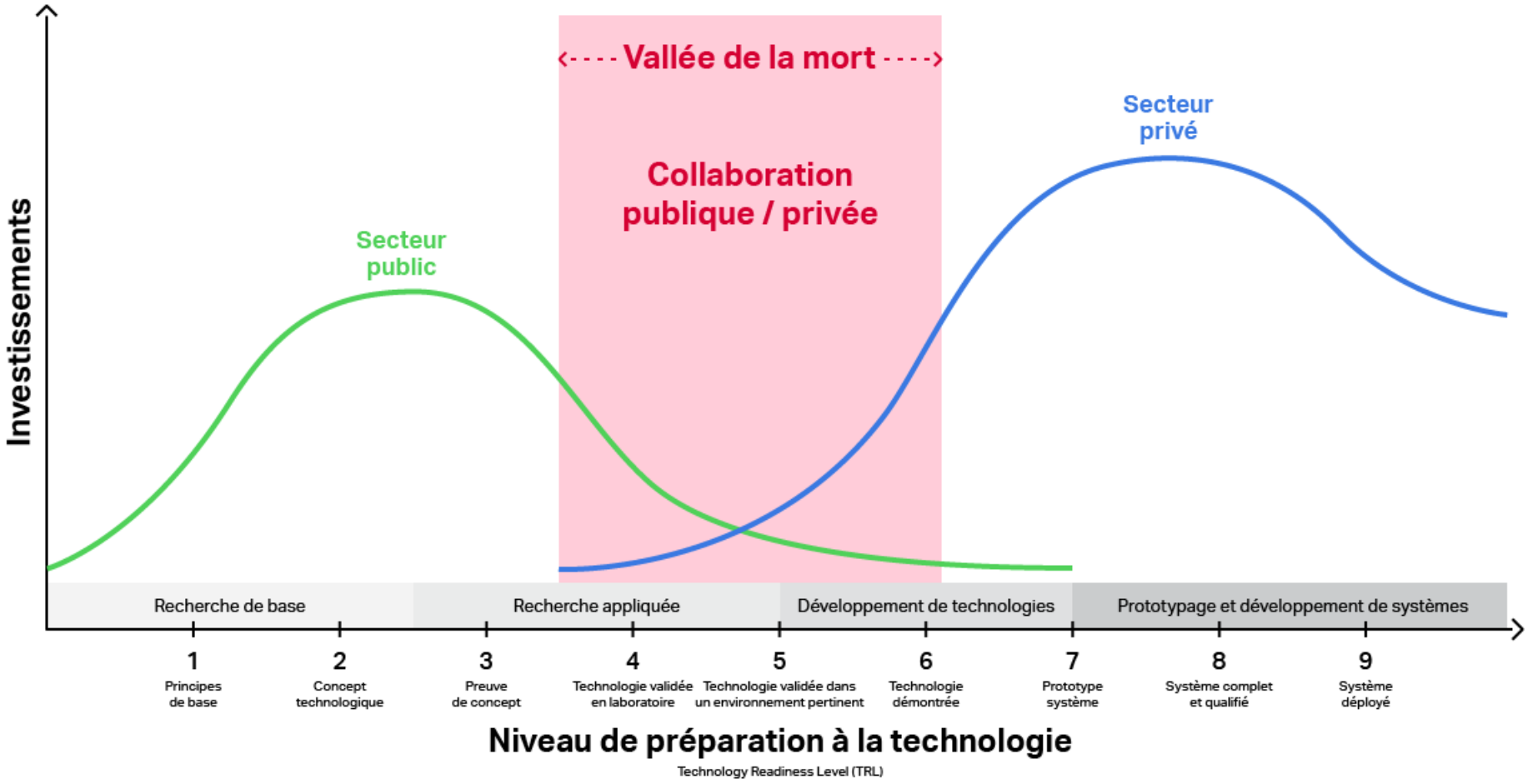
Planning réunions de groupe de travail par Défi

Date	Description
12/2022	Lancement groupe de travail
04-06/2023	Présentation des recherches et discussion sur les démonstrateurs
12/2023	Présentation des démonstrateurs
04-06/2024	Présentation des démonstrateurs finaux

Qui participe:

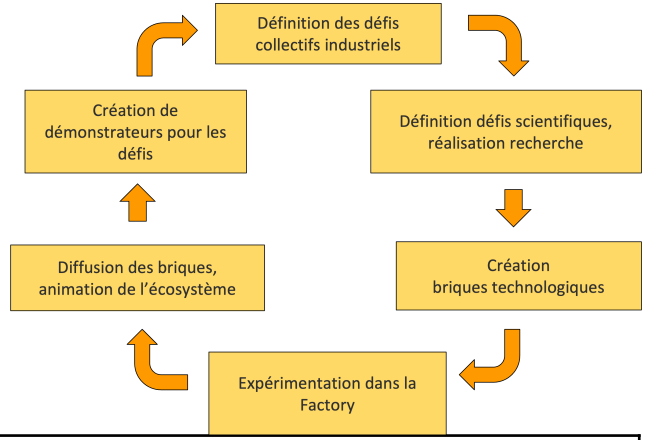
- Entreprises intéressées par le défi
- Responsable de défi
- Chercheurs contribuant au défi
- WSL

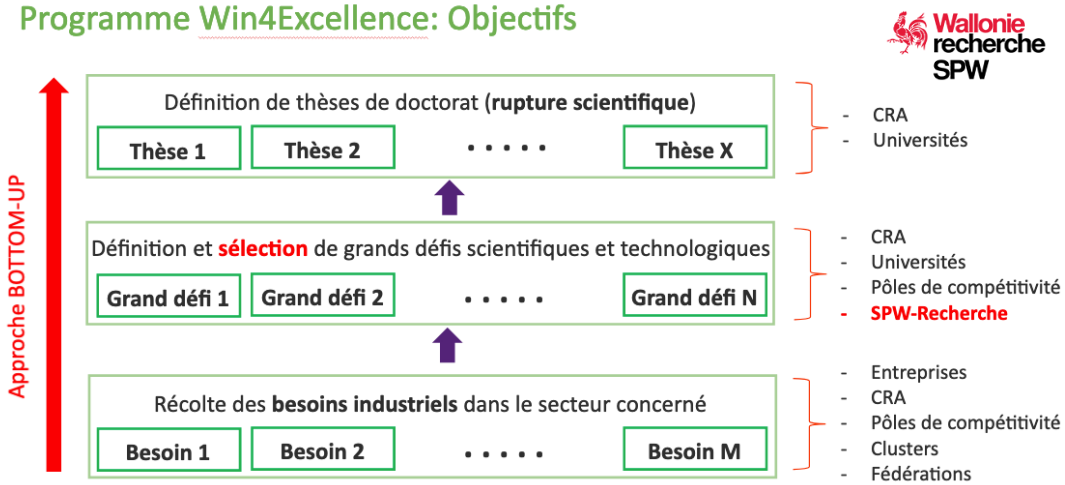
Merci de votre attention


Vallée de la mort
Collaboration publique / privée
Secteur public
Secteur privé
Investissements
Recherche de base
Recherche appliquée
Développement de technologies
Prototypage et développement de systèmes
1
Principes de base
2
Concept technologique
3
Preuve de concept
4
Technologie validée en laboratoire
5
Technologie validée dans un environnement pertinent
6
Technologie démontrée
7
Prototype système
8
Système complet et qualifié
9
Système déployé
Niveau de préparation à la technologie
Technology Readiness Level (TRL)

Projet CyberExcellence, Défis Collectifs Industriels, Factory

- Projet CyberExcellence
  - projet de recherche en cybersécurité, 01/01/2022, 18,9 millions de budget)
  - Partenaires : 5 universités + 2 CRA
- Défi Collectif Industriel
  - Récolte des besoins industriels dans le secteur concerné
  Identification des défis Collectif Industrie
- Factory
  - Production de briques technologiques
  - Validées dans des démonstrateurs





WP
WP1 : Rendre les systèmes résilients aux cyberattaques : phase de conception.
WP2 : Détection, Réponse, Réaction : Phase Dynamique
WP2 : RGPD et Open data : sécurité à la conception
WP3 : La protection et le partage des données au cœur des préoccupations
WP4 : Laboratoires d'expérimentation, de validation, et d'entraînement
WP5 : Factory et grands défis