



CentraleSupélec

université  
PARIS-SACLAY



CentraleSupélec

# ST5 - SYSTÈMES COMPLEXES ET CRITIQUES À LOGICIELS PRÉPONDÉRANTS

## INTRODUCTION À LA SÉQUENCE THÉMATIQUE

🎓 2A Cursus Ingénieurs - ST5 : Modélisation fonctionnelle et régulation

🏛️ CentraleSupélec - Université Paris-Saclay - 2024/2025



**Idir AIT SADOUNE**

[idir.aitsadoune@centralesupelec.fr](mailto:idir.aitsadoune@centralesupelec.fr)



# IDIR AIT SADOUNE

- **Docteur en Informatique** diplômé par l'**ENSMA** en **2010**.
  - **Thèse** sur la modélisation et la vérification des services par une approche basée sur le raffinement et sur la preuve.
- **Enseignant** au sein du département **informatique** de **CentraleSupélec**.
- **Chercheur** membre des pôles **Modèles** et **Preuve** du **LMF - Laboratoire Méthodes Formelles**.

# DISCUSSION AUTOUR DES ATTENTES DES ÉLÈVES



# PLAN

- ▶ Présentation générale de la ST
- ▶ Introduction, Contexte et Enjeux
- ▶ Présentation du cours spécifique
- ▶ Enseignement d'intégration
- ▶ Validation de la ST
- ▶ Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# PLAN

- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# LES RESPONSABLES DE LA ST



**Idir AIT SADOUNE**  
[idir.aitsadoune@centralesupelec.fr](mailto:idir.aitsadoune@centralesupelec.fr)

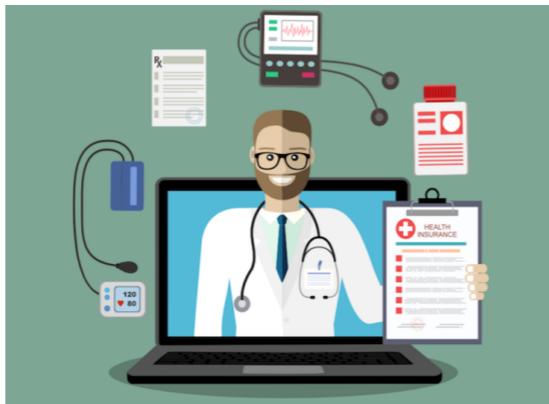


**Paolo BALLARINI**  
[paolo.ballarini@centralesupelec.fr](mailto:paolo.ballarini@centralesupelec.fr)

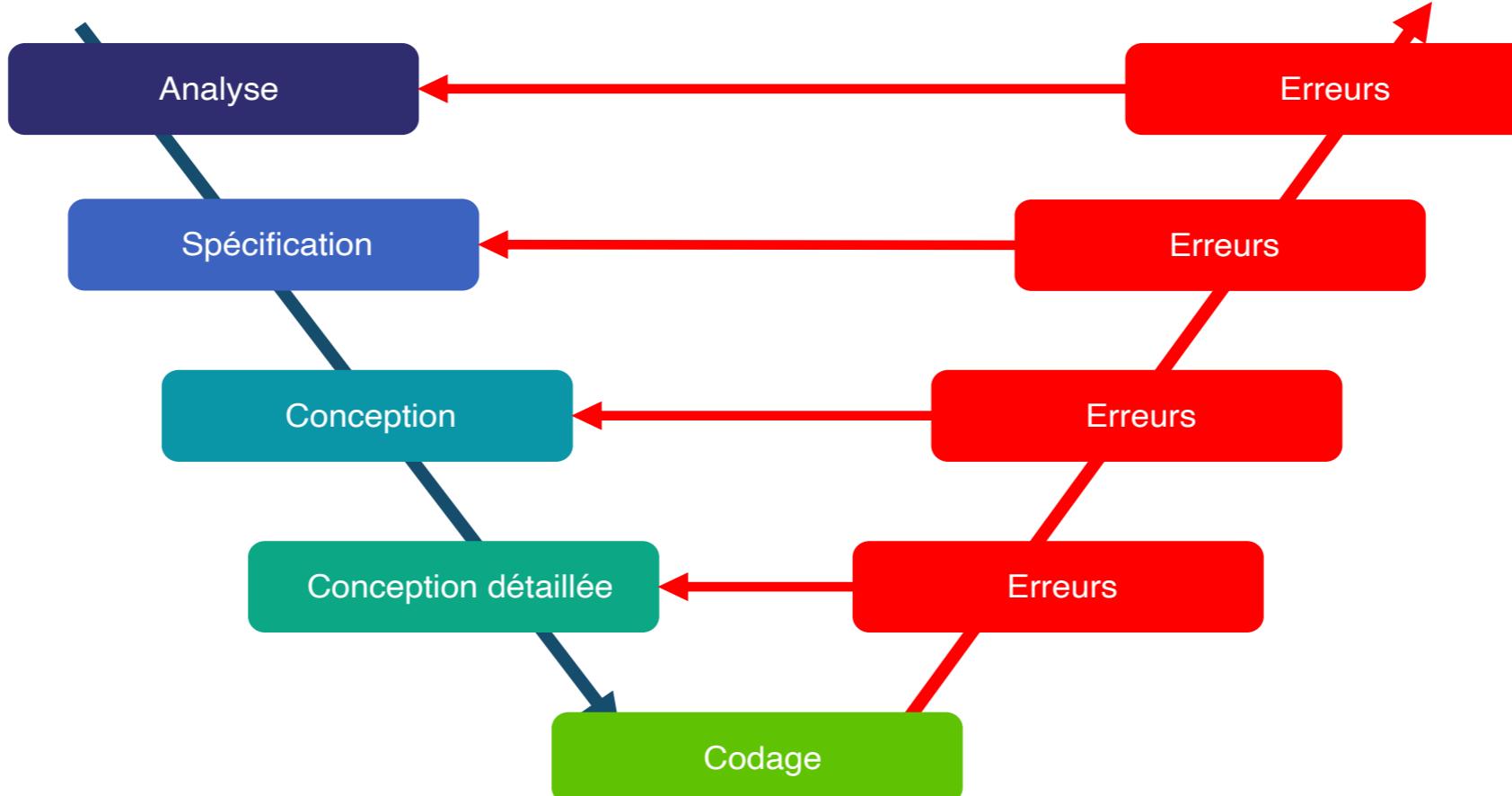


**Lina YE**  
[lina.ye@centralesupelec.fr](mailto:lina.ye@centralesupelec.fr)

# LE LOGICIEL INFORMATIQUE



# CYCLE DE DÉVELOPPEMENT



Des **erreurs** possibles à toutes les étapes du développement.

# LOGICIELS CRITIQUES

- Une défaillance dans un logiciel peut avoir des conséquences catastrophiques (humaines, financières, ...).
- Exemple du calculateur de bord d'Ariane 5  
➡ Vol 241/5101 du 25 janvier 2018



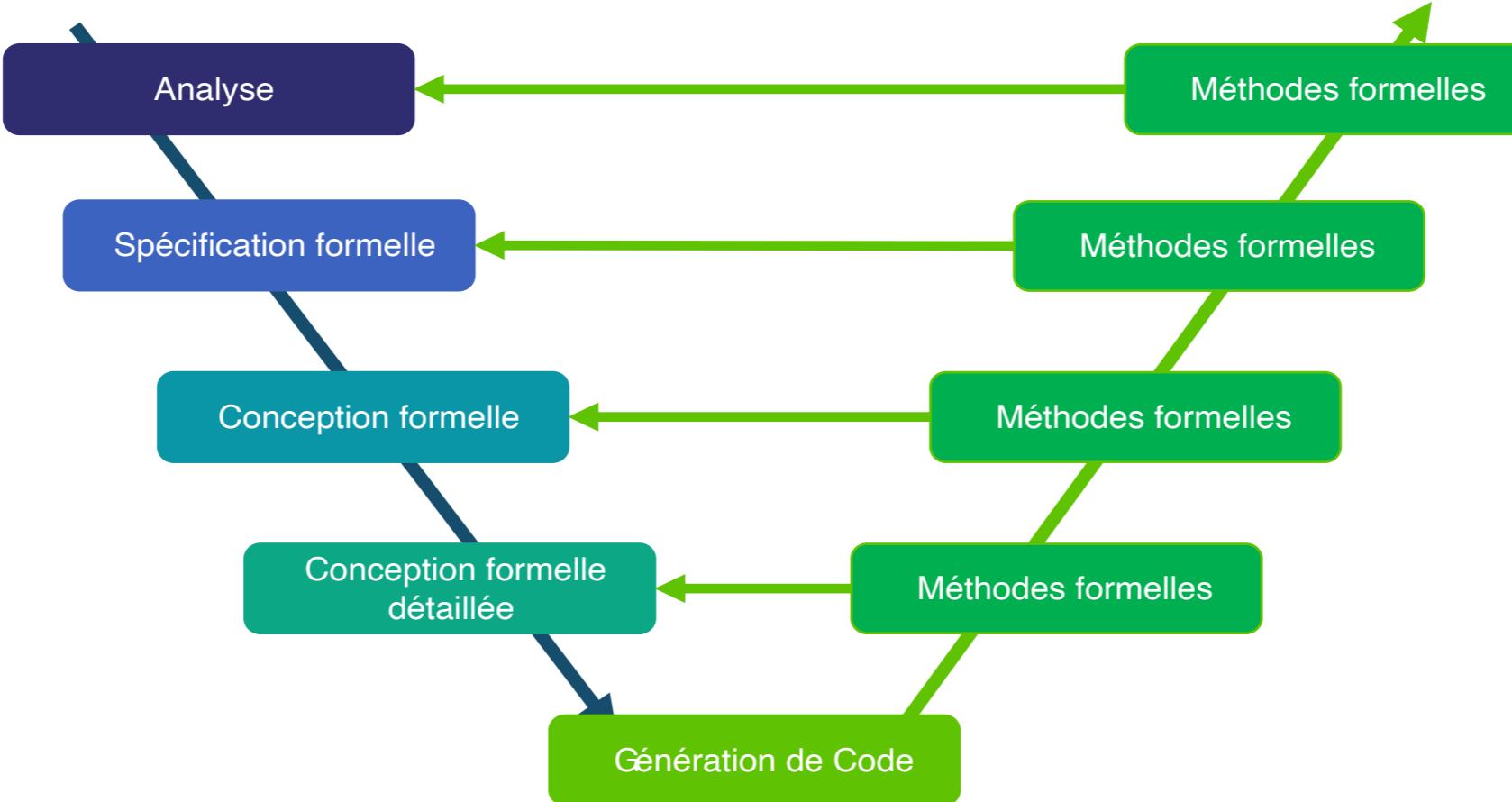
# SITUATIONS À ÉVITER !!!



# SOLUTIONS

- Les **règles et les techniques** de programmation.
- Le **support** des langages de programmation.
- Les **méthodologies de conception** et de développement.
- Le **test**.
- **Les méthodes formelles.**

# LA PLACE DES MÉTHODES FORMELLES



Utiliser les **méthodes formelles** dans **toutes les étapes**.

# LES MÉTHODES FORMELLES ET LA VÉRIFICATION

- **Les méthodes formelles**
  - ➡ Une **méthode d'ingénierie** pour le développement de systèmes basée sur des **concepts logiques et mathématiques** rigoureux.  
(**déterminer** ce que le logiciel est censé faire)
- L'activité de **vérification**
  - ➡ **Vérifier** qu'un système **répond aux exigences** identifiées dans sa **spécification** en utilisant **une méthode formelle**.  
(**prouver** que le logiciel fait ce qu'il est censé faire)
- **Spécification formelle**  $\Leftrightarrow$  **Vérification formelle**  $\Leftrightarrow$  **Synthèse formelle**

# CONCLUSION

Une **analyse** utilisant les **méthodes formelles** peut fournir la **preuve** que le système est complet et **correct vis à vis de ses exigences**.

# QUI RECOMMANDÉ LES MÉTHODES FORMELLES ?

- **Normes européennes**

L'utilisation de spécifications formelles seule rend les exigences non ambiguës.

- **Normes de l'aéronautique**

L'utilisation de méthodes formelles a pour but d'éliminer les erreurs de spécification, de conception et de codage lors du développement.

- **Normes du ferroviaire**

Pour les spécifications, des méthodes formelles sont recommandées car le modèle formel fournit précision, non ambiguïté et cohérence.

# EXEMPLES DE NORMES

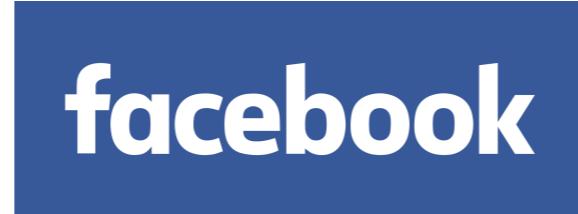
- Les **normes européennes EN 50126, EN 50128, EN 50129**
  - ➡ des **standards** utilisés dans le **domaine ferroviaire**.
  - ➡ requises pour les fournisseurs d'équipements de contrôle-commande.



# LES MÉTHODES FORMELLES RECOMMANDÉES

- Quelques **méthodes formelles** recommandées par les **normes** :
  - ⇒ "CSP, HOL, LOTOS, **Temporal Logic**, **B Method**, **Model Checking ...**"
  - ⇒ page 103 de la norme **EN 50128**

# QUI UTILISE LES MÉTHODES FORMELLES?

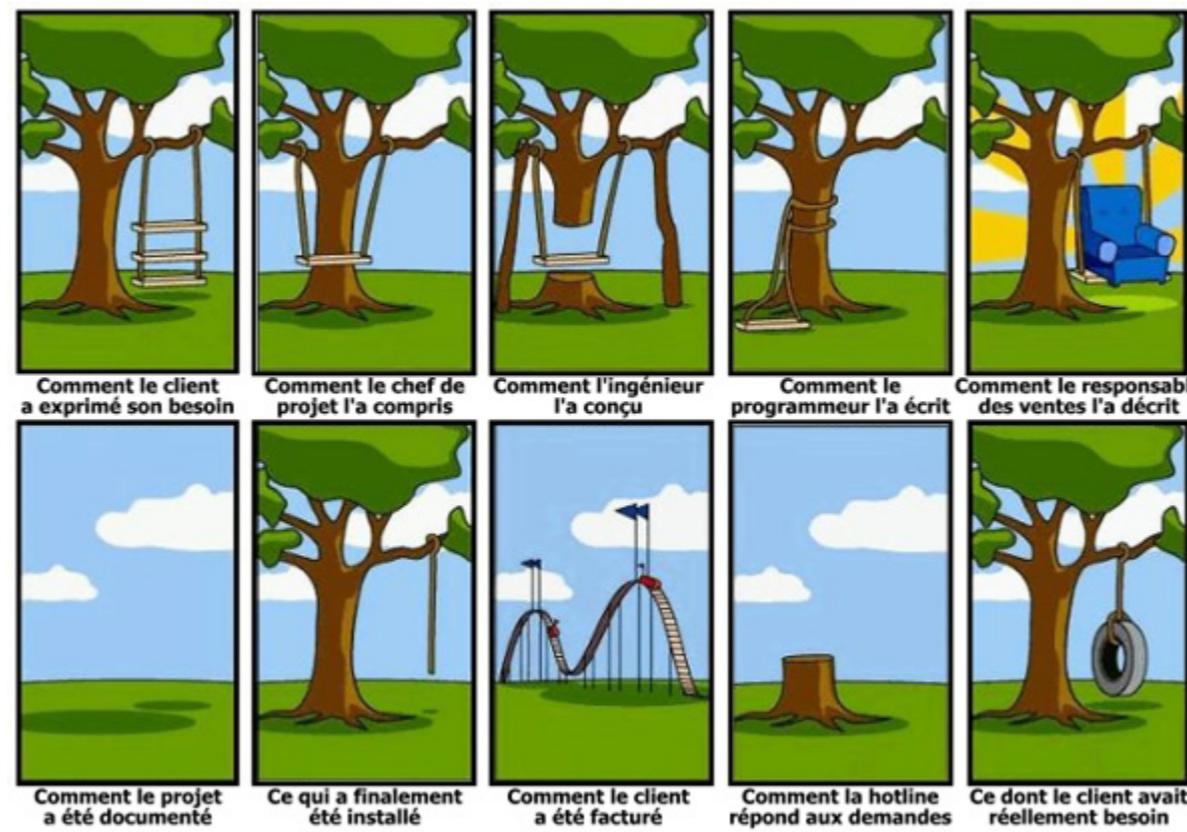


# EVALUATION ASSURANCE LEVEL (EAL)

- **7 niveaux d'assurance** d'évaluation selon [les critères communs](#)
  - **EAL1** : testé fonctionnellement
  - **EAL2** : testé structurellement
  - **EAL3** : testé et vérifié méthodiquement
  - **EAL4** : conçu, testé et vérifié méthodiquement
  - **EAL5** : conçu de façon semi-formelle et testé
  - **EAL6** : conception vérifiée de façon semi-formelle et système testé
  - **EAL7** : conception vérifiée de façon formelle et système testé
- **Les applications civiles** : les EAL sont généralement de 1 à 4 (4+).
- **Les applications militaires** : les EAL sont de 5 à 7.

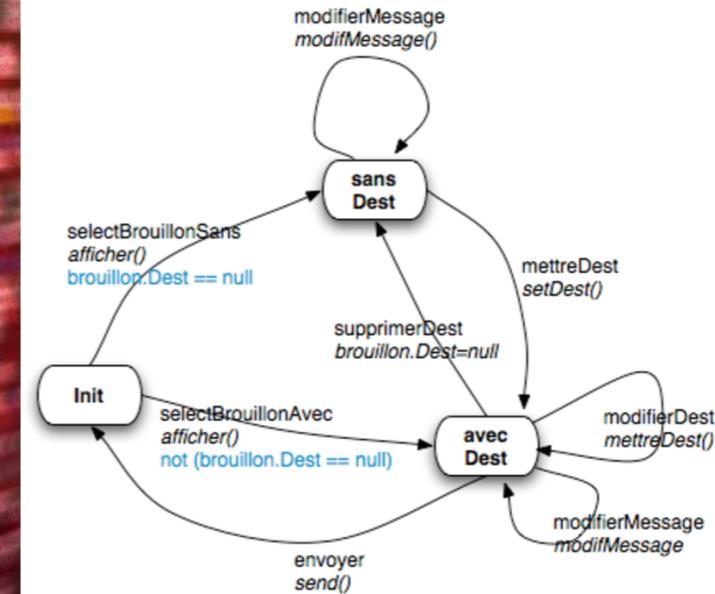
# QUELQUES MYTHES

- L'utilisation des méthodes formelles **produit un logiciel parfait ?**
  - ➡ non-sens, une spécification formelle est un modèle du monde réel
  - ➡ peut inclure des erreurs, des omissions et des malentendus



# QUELQUES MYTHES

- Utiliser les méthodes formelles  $\approx$  faire de la preuve de programme ?
  - ➡ la modélisation d'un système est valable sans vérification de programmes
  - ➡ la spécification formelle force à une analyse détaillée du système



# QUELQUES MYTHES

- Les méthodes formelles que pour **les systèmes critiques** ?
  - ➡ l'expérience industrielle montre que les coûts de développement sont réduits pour tous les types de systèmes.  
(IHM multimodales, microservices, validation de données, ...)



# QUELQUES MYTHES

- Les méthodes formelles sont uniquement pour **les mathématiciens** ?  
➡ non-sens, les mathématiques employées sont élémentaires.

$$\text{tg } \alpha = \frac{\sin \alpha}{\cos \alpha} = \frac{a}{c}$$
$$\frac{a}{\sin \alpha} = \frac{b}{\sin \beta} = \frac{c}{\sin \gamma} = 2R$$
$$\text{tg}(\alpha - \beta) = \frac{\text{tg} \alpha - \text{tg} \beta}{1 + \text{tg} \alpha \cdot \text{tg} \beta}$$
$$f'(x) = \lim_{x \rightarrow 0} \frac{f(x+h) - f(x)}{h}$$

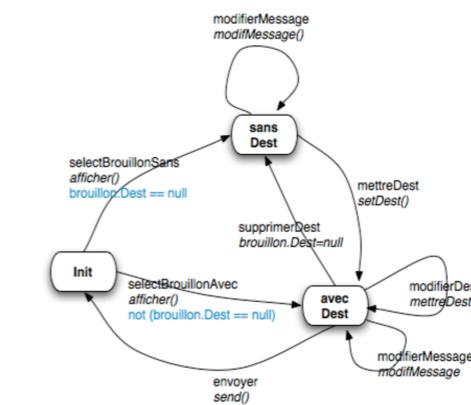
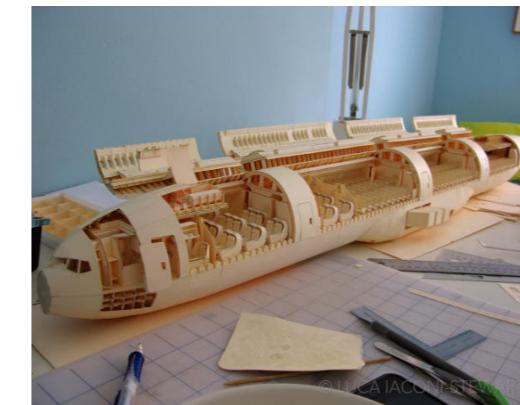
# QUELQUES MYTHES

- Les méthodes formelles **augmentent les coûts de développement ?**  
➡ non-prouvé, il y a un déplacement des coûts vers les premières étapes.

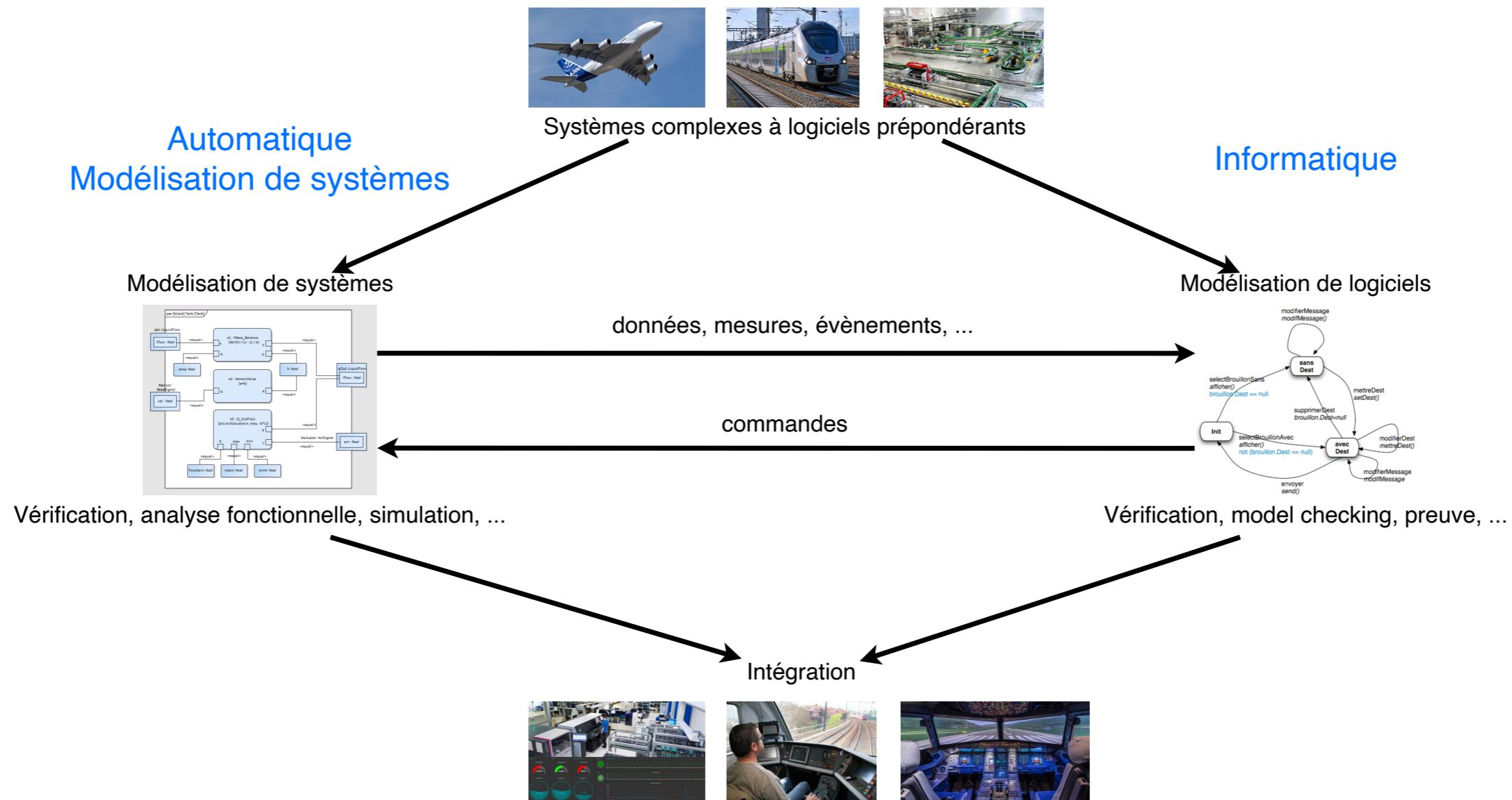


# QUELQUES MYTHES

- Les clients **ne peuvent pas comprendre** les spécifications formelles.  
➡ il faut les paraphraser en langage naturel, ou utiliser le prototypage.

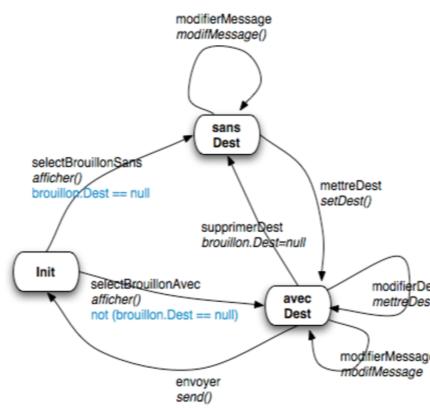


# LE CADRE DE LA ST



# L'OBJECTIF DE LA ST

Comment exprimer (modéliser) et vérifier  
les propriétés comportementales des systèmes critiques ?



Cette ST va vous aider à répondre à cette question !!!

# PLAN

- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# PLANNING

Lundi 16 septembre 2024 - Amphi sa.108, Bouygues

**08h15 - 09h45** Présentation de la séquence thématique

---

Idir AIT-SADOUNE (CentraleSupélec)

**10h00 - 11h30** Séminaire

---

Guillaume GIRAUD (RTE)

# PLANNING

Lundi 23 septembre 2024 - Amphi sa.108, Bouygues

**08h15 - 09h45 Séminaire**

---

Michel BATTEUX (Systemic Intelligence)

**10h00 - 11h30 Séminaire**

---

Carlos BERNAD & Lucien PEREZ (IKOS Consulting)

# PLANNING

Mardi 24 septembre 2024 - Amphi sa.108, Bouygues

**08h15 - 09h45** Présentation des EIls

---

Idir AIT-SADOUNE (CentraleSupélec)

**10h00 - 11h30** Séminaire

---

Thierry LECOMTE (ClearSy)

# LA SYNTHÈSE DES SÉMINAIRES

- Rédaction d'un **résumé** de **10 lignes maximum** par **séminaire**.
  - à saisir sur **la page de la ST** dans **EDUNAO**,
  - **4 résumés** attendus pour chaque étudiant,
  - une **évaluation** sera effectuée par l'enseignant,
  - une attention particulière sera portée à la **clarté des résumés**.
- Validation du module **Contexte et Enjeux** :
  - **présence obligatoire** à tous les séminaires,
  - rédaction des **4 résumés sur EDUNAO**,
  - permet de valider la compétence **C2**
    - ➡ développer ses compétences dans un domaine d'ingénieur et dans un métiers
- Rendu dans **EDUNAO** avant le **mercredi 09/10/2024 à 23h59**

# PLAN

- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# LE PROGRAMME

## CONCEPTION ET VÉRIFICATION DE SYSTÈMES CRITIQUES

### Les logiques temporelles

**3 CMs, 2 TDs (5 × 1h30)**

---

Idir AIT SADOUNE (CentraleSupélec)

### Le Model Checking

**1 CMs, 1 TDs (2 × 1h30)**

---

Paolo BALLARINI (CentraleSupélec)

### Les automates temporisés

**2 CMs, 2 TDs, 1 TP (6 × 1h30)**

---

Lina YE (CentraleSupélec)

### Les modèles stochastiques

**2 CMs, 2 TDs, 1 TP (6 × 1h30)**

---

Paolo BALLARINI (CentraleSupélec)

# ORGANISATION DU COURS

- **Date de début** : lundi 16/09/2024 à 15h30 / **Amphi sa.108, Bouygues.**
  - **Cours** → en présentiel
  - **TD** → en présentiel
  - **TP** → en présentiel obligatoire (travail à finir à la maison et **à rendre**)
- Polycopie, slides, énoncés des TD/TP, corrections des TD/TP  
**en versions PDF** disponibles dans **Edunao**.
- Polycopie **en version papier** disponible
- Le polycopie contient plus d'informations que ce qui sera vu en cours.

# PLAN

- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# LES EI - ENSEIGNEMENTS D'INTÉGRATION

Présentation des sujets et des détails de l'organisation des EIls  
le **mardi 24/09/2024** à *8h15*.

# PLAN

- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# VALIDATION DE LA ST

- La **ST5** valide une Unité d'Enseignement (**UE**) **Séquence Thématique** dédiée à **la modélisation fonctionnelle et la régulation**.
- L'évaluation est constituée des activités suivantes :
  - **modules contexte et enjeux** : 0.2 ECTS,
  - **cours automatique et contrôle** : 2.5 ECTS,
  - **cours modélisation système** : 2 ECTS,
  - **cours spécifique** : 2.5 ECTS,
  - **enseignement d'intégration (EI)** : 1.8 ECTS.
- Pour **valider une UE**, un élève doit obtenir **une note  $\geq 10/20$**  à **chacune des activités** constituant l'UE.
- L'**EI** est **un cas particulier** et doit être validé par **une note  $\geq 12/20$** .

# EVALUATIONS

- **Module contexte et enjeux**
  - la présence et l'évaluation des résumés de séminaires.
- **Cours spécifique**
  - la présence et la réalisation des deux TP
  - l'**examen écrit** prévu le **Jeudi 14/11/2024**.
  - les sujets d'examens seront en français et en anglais.
  - les élèves peuvent composer dans la langue de leur choix.
  - le contrôle final aura une durée de **1h30**.
- **Enseignement d'Intégration**
  - la note sera détaillée lors de la présentation des **Els**.

# L'ÉVALUATION DES COMPÉTENCES

La **ST5** évalue les compétences **C1, C2, C4, C6** et **C7**.

- **Module contexte et enjeux**
  - **C2** → Développer ses compétences dans un domaine d'ingénieur et dans un métiers
- **Cours spécifique**
  - **C1** → Analyser, concevoir et réaliser des systèmes complexes
    - **C1.2** → l'examen écrit : utiliser et développer les modèles adaptés, choisir la bonne échelle de modélisation et les hypothèses pertinentes
    - **C1.4** → le TP : spécifier, réaliser et valider un système complexe
- **Enseignement d'Intégration**
  - **C4** : Avoir le sens de la création de valeur pour son entreprise et ses clients
  - **C6** : Être opérationnel, responsable et innovant dans le monde numérique
  - **C7** : Savoir convaincre

# ORGANISATION DES RATTRAPAGES

- **Module contexte et enjeux**
  - si un résumé n'est pas rendu → c'est FAIL en C2.
  - si absence non justifiée à un séminaire → c'est FAIL en C2.
  - si FAIL → un oral de 15 minutes est organisé.
- **Cours spécifique**
  - si le TP n'est pas rendu → c'est FAIL en C1.
  - si absence non justifiée au TP → c'est FAIL en C1.
  - si la note examen écrit  $\leq 10$  → c'est FAIL en C1.
  - si la note examen écrit  $\leq 7$  → un rattrapage est programmé.
- **Enseignement d'Intégration**
  - si la note  $< 12$  → un rattrapage est programmé.
  - la validation des  $C_i$  est définie par le responsable de l'EI.

# PLAN

- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

# DOMINANTE INFORMATIQUE ET NUMÉRIQUE EN 3A

Mention : **Science du Logiciel**

<https://wdi.centralesupelec.fr/infonum-sl/>

**Responsable** : Frédéric BOULANGER

[frederic.boulanger@centralesupelec.fr](mailto:frederic.boulanger@centralesupelec.fr)

# MERCI

[Version PDF des slides](#)

[Retour à l'accueil - Retour au plan](#)