

# ST58 - SYSTÈMES COMPLEXES ET CRITIQUES À LOGICIELS PRÉPONDÉRANTS

## INTRODUCTION À LA SÉQUENCE THÉMATIQUE

🎓 2A Cursus Ingénieurs - ST5 : Modélisation fonctionnelle et régulation  
🏛️ CentraleSupélec - Université Paris-Saclay - 2025/2026



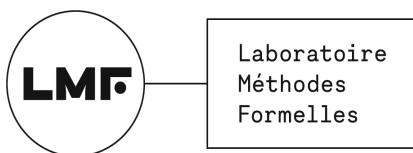
**Idir AIT SADOUNE**

[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 - Université Paris-Saclay](#).
- Chercheur membre des **pôles Modèles** et **Preuve** du [LMF - Laboratoire Méthodes Formelles](#).



# 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)

# DISCUSSION AUTOURS DU CONTENU DE LA ST ET DES ATTENTES DES ÉTUDIANTS



# 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

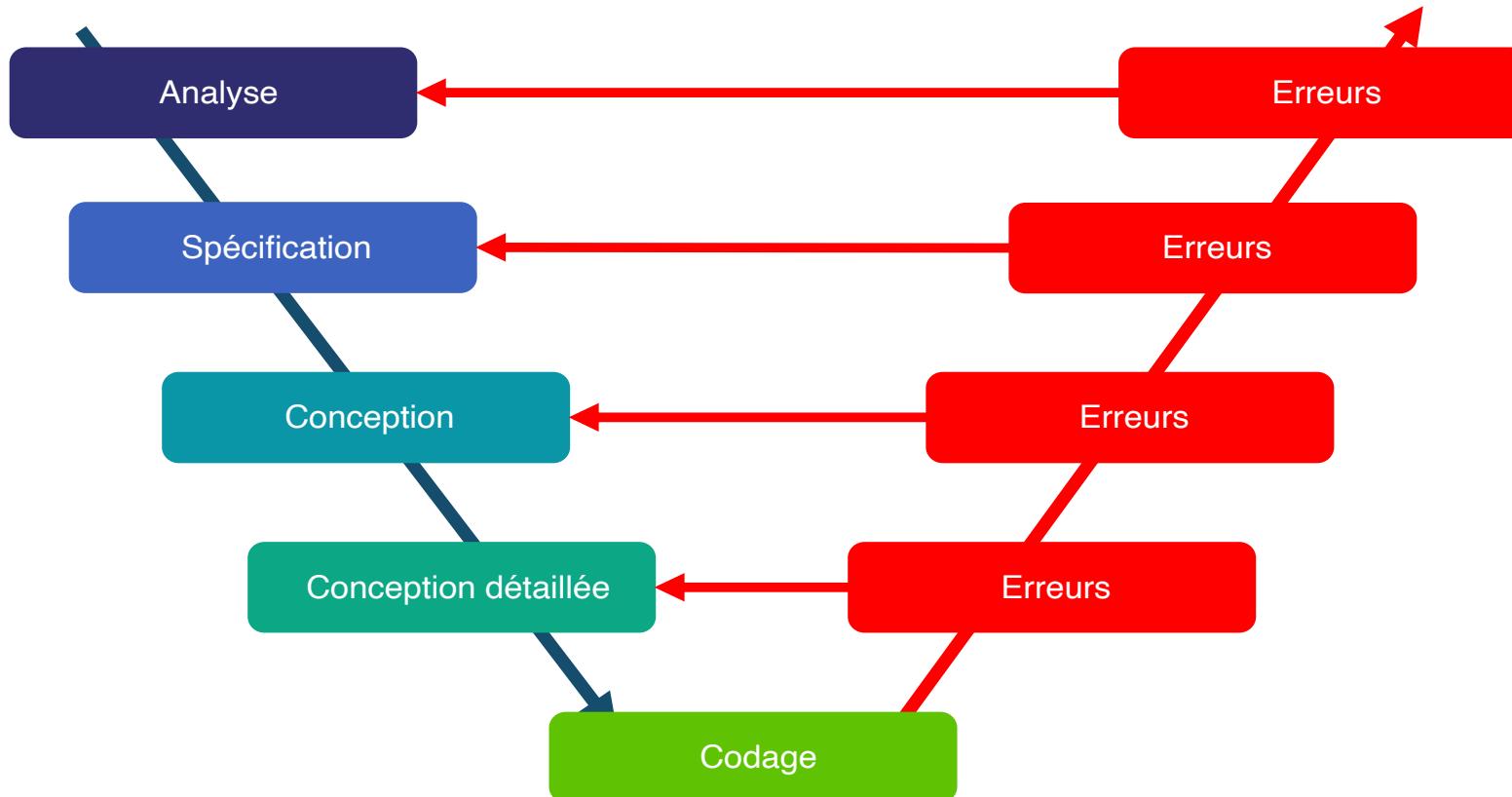
- Présentation générale de la ST
- Introduction, Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

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

# 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 501 du 4 juin 1996

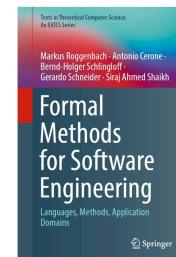


# SITUATIONS À ÉVITER !!!



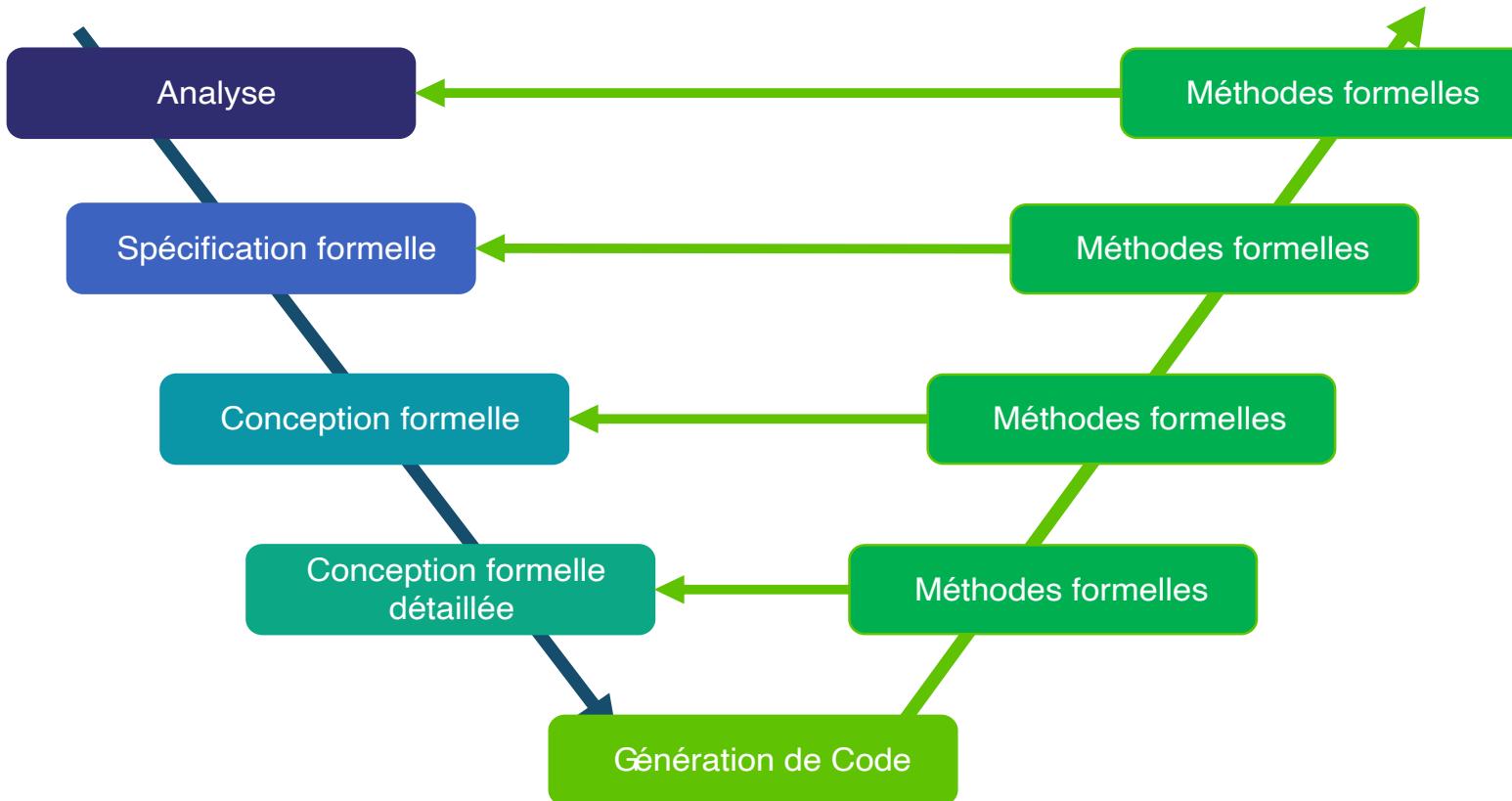
# SOLUTIONS

- 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
  - ➡ méthodes d'ingénierie basées sur des approches mathématiques utilisées pour développer et analyser des systèmes (logiciels).
  - ➡ démarche globale (langages et outils de vérification).



**Formal Methods for Software Engineering**  
Languages, Methods, Application Domains  
Springer 2022

# LA PLACE DES MÉTHODES FORMELLES



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

# SPÉCIFICATION, CONCEPTION ET VÉRIFICATION

- La spécification formelle → description rigoureuse et non ambiguë du comportement attendu d'un système (logiciel).
  - ➡ modèle mathématique décrivant ce que doit faire le système (logiciel).
  - ➡ modélisation par un langage mathématique (syntaxe, logique, sémantique...).
- La conception formelle → description rigoureuse et non ambiguë de la réalisation du système (logiciel).
  - ➡ modèle mathématique décrivant la construction du système (logiciel).
  - ➡ modélisation par un langage mathématique (syntaxe, logique, sémantique...).
- La Vérification formelle → démontrer mathématiquement qu'un système (logiciel) respecte les exigences identifiées dans la spécification.
  - ➡ démonstration que la conception correspond bien à la spécification.
  - ➡ simulation, preuve de théorèmes, model checking...

## 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 ?

Secteur/Domaine	Norme principale	Brève description
Ferroviaire (rail)	EN 50128 → EN 50716 (2023)	Logiciels de contrôle : SIL ; agile, modélisation, IA/ML (2023)
Ferroviaire (rolling stock)	EN 50657 (2017)	Logiciels embarqués sur matériel roulant
Ferroviaire (cybersécurité)	CLC/TS 50701 (2021)	Spécification pour sécurité IT/OT (données/opérations) dans le ferroviaire
Aéronautique	DO-178C/ED-12C	Logiciels avioniques - cycle complet et certification
Industrie générique/sécurité	IEC 61508	Cadre générique pour sécurité fonctionnelle (cycle de vie + SIL)
Automobile	ISO 26262	Sécurité fonctionnelle pour véhicules
Dispositifs médicaux	IEC 62304 (EN 62304)	Logiciel médical : cycle de vie, maintenance, gestion des risques

# EXEMPLES DE NORMES → FERROVIAIRE

- EN 50128 Software for railway control and protection system
  - norme européenne très connue pour les logiciels critiques dans le ferroviaire
- EN 50657:2017
  - logiciel embarqué dans le matériel roulant (rolling stock)
- EN 50716:2023 (remplaçant EN 50128)
  - introduit des approches itératives (agile), l'usage de modèles (UML, SysML), voire l'intégration de l'IA/ML dans le cycle de développement
- CLC/TS 50701:2021
  - spécification axée sur la cybersécurité dans les applications ferroviaires



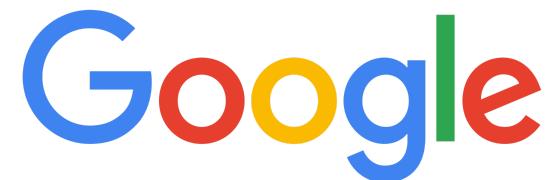
# EXEMPLES DE NORMES → FERROVIAIRE

## 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**



## QUELQUES ACTEURS UTILISANT LES MÉTHODES FORMELLES



# EVALUATION ASSURANCE LEVEL (EAL) SELON LES CRITÈRES COMMUNS

- **EAL1** → testé fonctionnellement (les risques sont faibles)
  - Vérifications basiques, sans grande analyse de conception.
- **EAL2** → testé structurellement (une certaine sécurité sans forte menace)
  - Analyse de conception limitée + vérifications fonctionnelles.
- **EAL3** → testé et vérifié méthodiquement (des risques modérés)
  - Vérification méthodique de la conception et des tests
- **EAL4** → conçu, testé et vérifié méthodiquement (banques, administrations...)
  - Analyse approfondie de la conception, documentation détaillée, vérifications...
- **EAL5** → conçu de façon semi-formelle et testé (systèmes sensibles aux attaques)
  - Introduction de méthodes semi-formelles dans la conception.
- **EAL6** → conception vérifiée de façon semi-formelle et système testé (défense)
  - Analyse poussée avec vérifications de sécurité avancées.
- **EAL7** → conception vérifiée formellement et système testé (produits militaires)
  - Niveau le plus strict : preuves formelles et exhaustives.

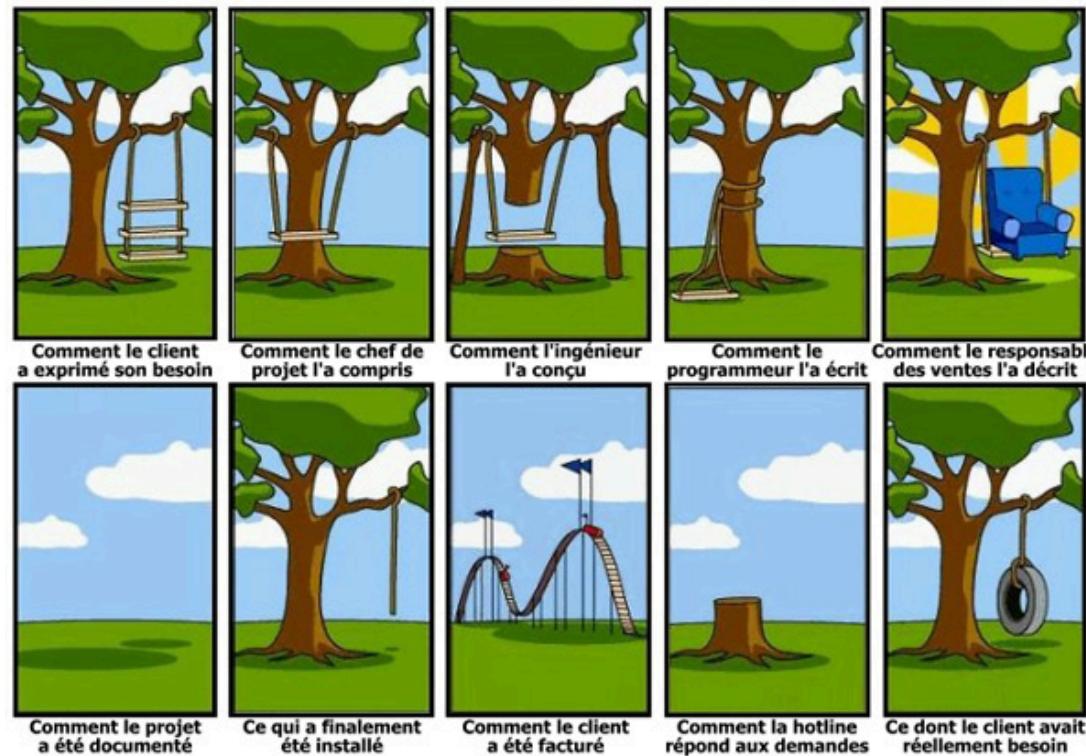
# EVALUATION ASSURANCE LEVEL (EAL) SELON LES CRITÈRES COMMUNS

## EN PRATIQUE

- **EAL4** → est souvent le niveau maximum recherché dans le commerce (bon compromis coût/sécurité).
- **EAL5 à EAL7** → concernent des systèmes de défense, gouvernementaux ou infrastructures critiques.

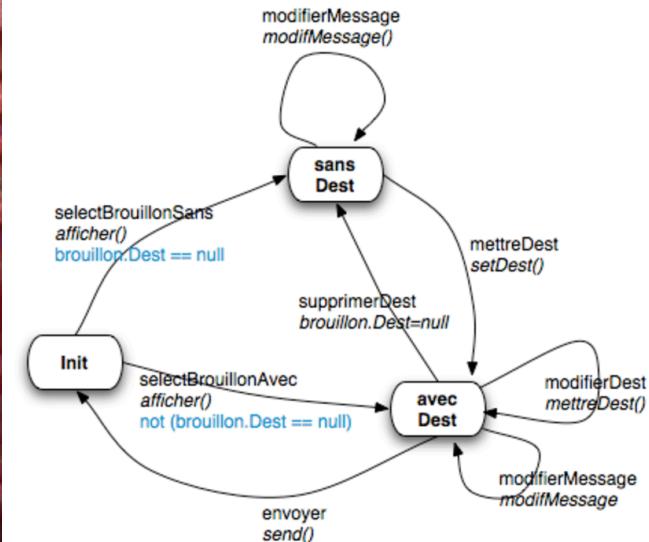
# QUELQUES MYTHES

- 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.

$$\begin{aligned} \operatorname{tg}\alpha \operatorname{ctg}\alpha &= 1 & \cos^2 \alpha &= \sec^2 \alpha & f'(x) &\equiv \lim_{x \rightarrow 0} \frac{f(x+h) - f(x)}{h} \\ \frac{a}{\sin \alpha} &= \frac{b}{\sin \beta} = \frac{c}{\sin \gamma} = 2R & 2 \sin^2 \alpha &= 1 + \cos 2\alpha & \cos 2\alpha &= 2 \cos^2 \alpha - 1 \\ (-a) \operatorname{tg}(\alpha - \beta) &= \frac{\operatorname{tg}\alpha - \operatorname{tg}\beta}{1 + \operatorname{tg}\alpha \operatorname{tg}\beta} & \log_b a &= \frac{\log_a b}{\log_a c} & \log_b c &= \frac{\log_a c}{\log_a b} \end{aligned}$$

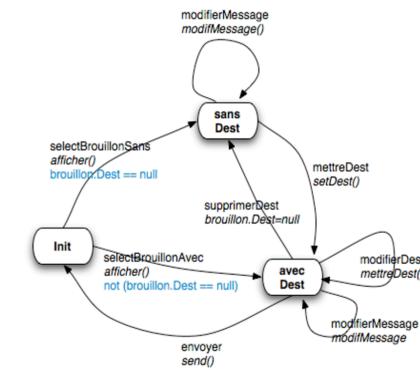
# QUELQUES MYTHES

- Les méthodes formelles **augmentent les coûts de développement ?**  
➡ **non-prouv **, il y a un d placement des coûts vers les premières t pes.

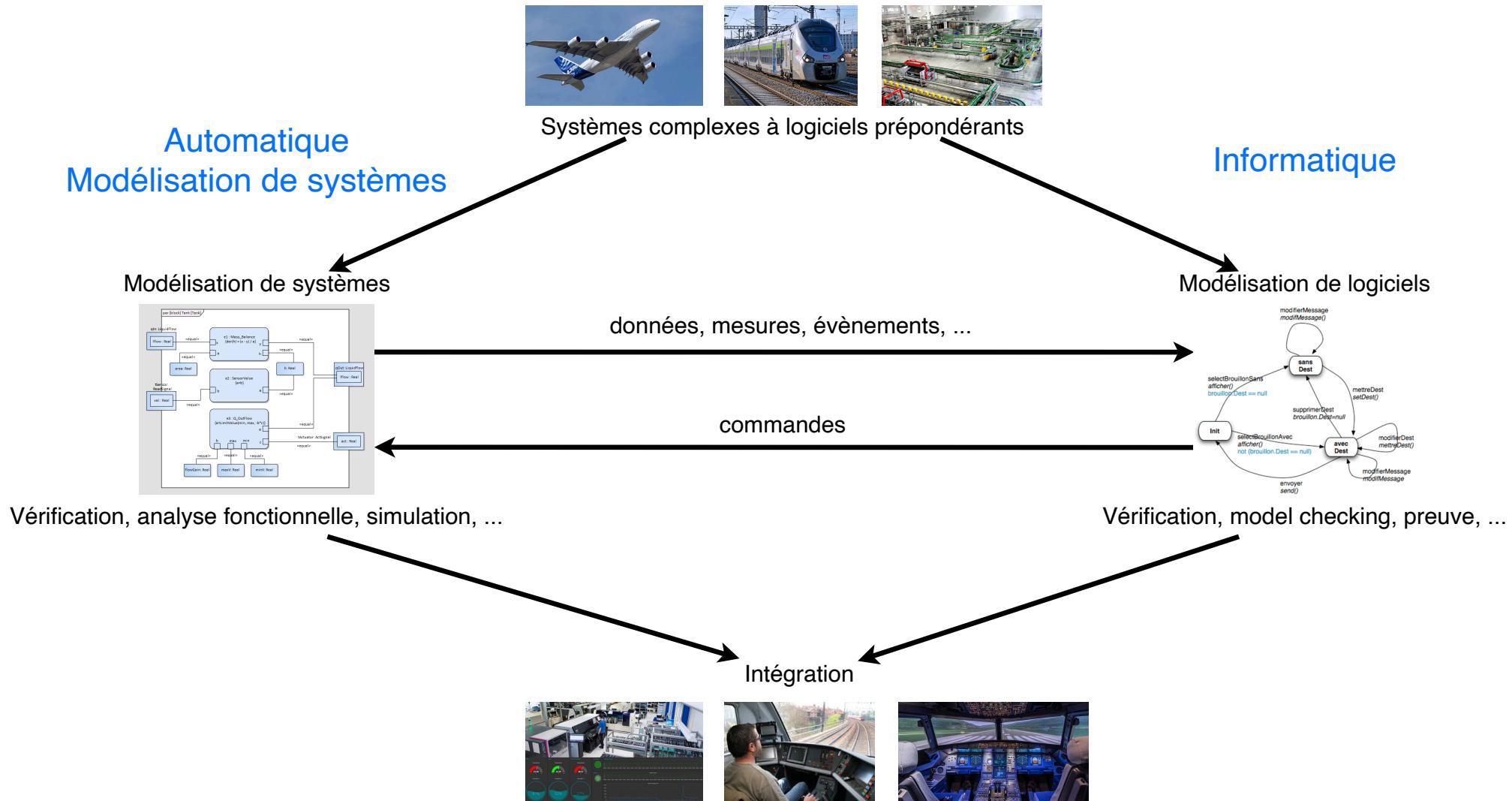


# QUELQUES MYTHES

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

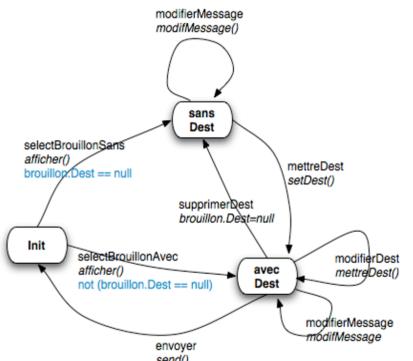


# LE CADRE DE LA ST



# 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 !!!

# L'OBJECTIF DE LA ST EST-IL CLAIRE POUR TOUT LE MONDE ?



# 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 15 septembre 2025 - Amphi sa.108, Bouygues

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

---

Idir AIT-SADOUNE (CentraleSupelec)

**10h00 - 11h30** Séminaire

---

Guillaume GIRAUD (RTE)

# PLANNING

Lundi 22 septembre 2025 - Amphi sa.108, Bouygues

**08h15 - 09h45 Séminaire**

---

Michel BATTEUX (Systemic Intelligence)

**10h00 - 11h30 Séminaire**

---

Carlos BERNAD & Lucien PEREZ (IKOS Consulting)

# PLANNING

Mardi 23 septembre 2025 - Amphi sa.108, Bouygues

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

---

Idir AIT-SADOUNE (CentraleSupelec)

**10h00 - 11h30** Séminaire

---

Émeric TOURNIAIRE (ClearSy)

# LA SYNTHÈSE DES SÉMINAIRES

- Rédaction d'un **résumé** de **10 lignes maximum** pour chaque **séminaire**.
  - à téléverser sur **la page de la ST** disponible sur **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,
  - disponibilité des **4 résumés sur EDUNAO** pour chaque étudiant,
  - validation de la compétence **C2** :  
*"développer ses compétences dans un domaine d'ingénieur et dans un métiers"*

Disponibilité des résumés sur **EDUNAO** avant le **mercredi 08/10/2025 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** Idir AIT SADOUNE (CentraleSupélec)

**3 CMs, 2 TDs (5 × 1h30)**

**Le Model Checking** Paolo BALLARINI (CentraleSupélec)

**1 CMs, 1 TDs (2 × 1h30)**

**Les automates temporisés** Lina YE (CentraleSupélec)

**2 CMs, 2 TDs, 1 TP (6 × 1h30)**

**Les modèles stochastiques** Paolo BALLARINI (CentraleSupélec)

**2 CMs, 2 TDs, 1 TP (6 × 1h30)**

# ORGANISATION DU COURS

- Date de début → lundi 15/09/2025 à 15h30.
  - Cours → vérifier régulièrement votre EDT
  - TD → présence recommandée
  - TP → présence obligatoire (**TP noté** 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 après sondage sur les demandes
  - 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 Els  
le **mardi 23/09/2025 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 13/11/2025 à 8h00** (une durée de **1h30**).
  - les sujets d'examens seront en français et en anglais.
  - les élèves peuvent composer dans la langue de leur choix.
- **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<sub>i</sub>** 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](#)