

# 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.

# IDIR AIT SADOUNE



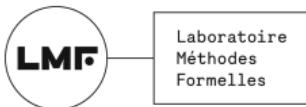
- Docteur en Informatique diplômé par l'ENSMA [en 2010](#).
  - Thèse [sur la modélisation et la vérification des services](#) par une approche basée sur le [raffinement](#) et sur la [preuve](#).
- Enseignant au sein du département [informatique](#) de CentraleSupélec - Université Paris-Saclay [.](#)



# 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



# OUTLINE

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

[Back to the begin](#) - [Back to the outline](#)

# OUTLINE

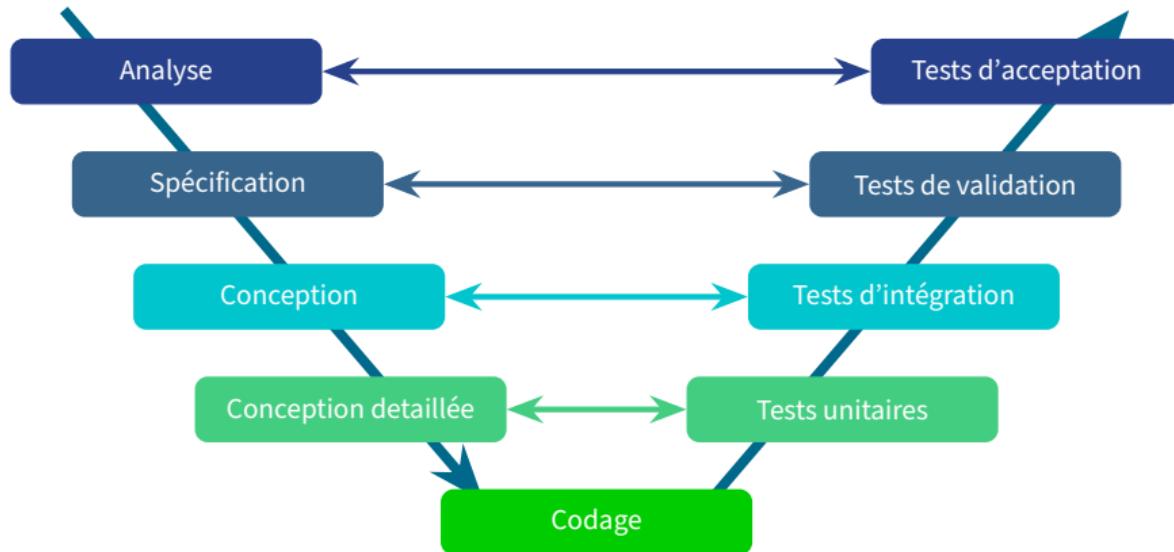
- ▶ Présentation générale de la ST
- ▶ Introduction, Contexte et Enjeux
- ▶ Présentation du cours spécifique
- ▶ Enseignement d'intégration
- ▶ Validation de la ST
- ▶ Pour aller plus loin

[Back to the begin](#) - [Back to the outline](#)

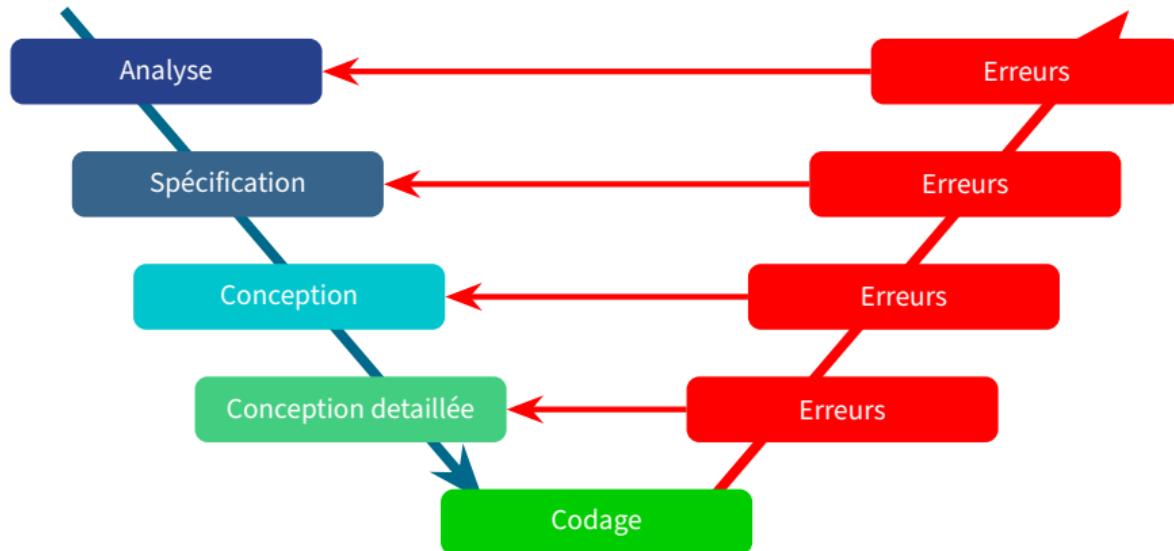
# LE LOGICIEL INFORMATIQUE



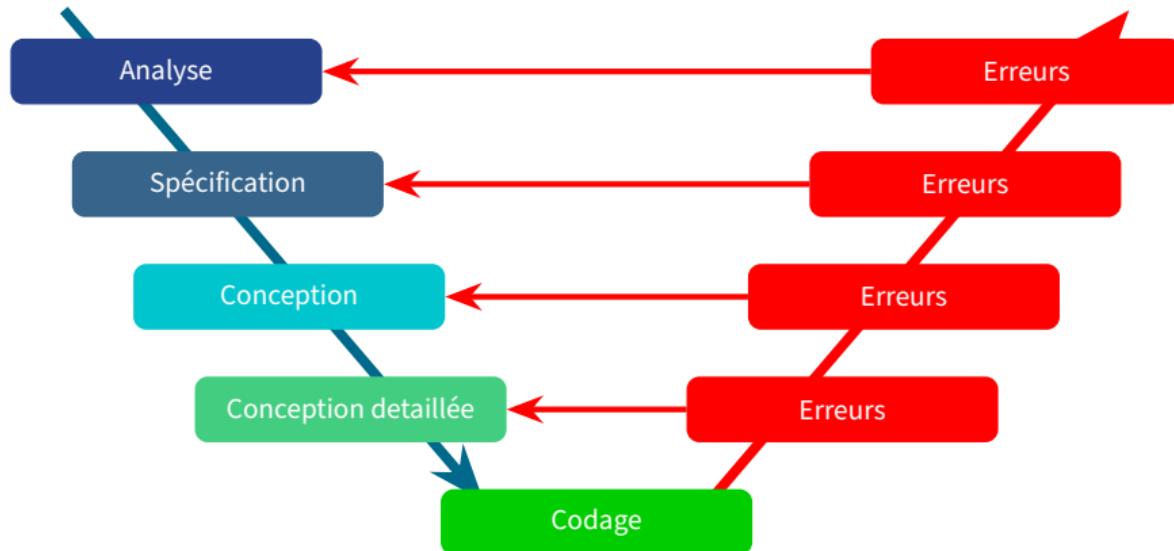
# CYCLE DE DÉVELOPPEMENT



# CYCLE DE DÉVELOPPEMENT



# 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, ...).

# 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



# SOLUTIONS

- Les règles et les techniques de programmation.



# SOLUTIONS

- Les **règles** et les **techniques** de programmation.
- Le **support** des langages de programmation.



# SOLUTIONS

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



# SOLUTIONS

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



# 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**.



# 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.**



# 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).



# 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).



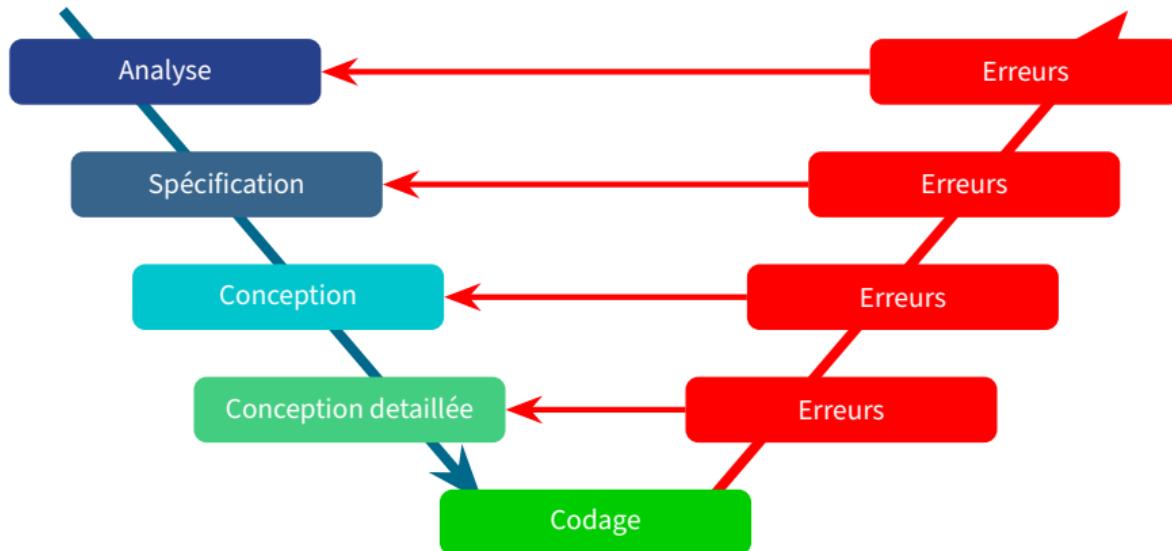
# SOLUTIONS

- 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).

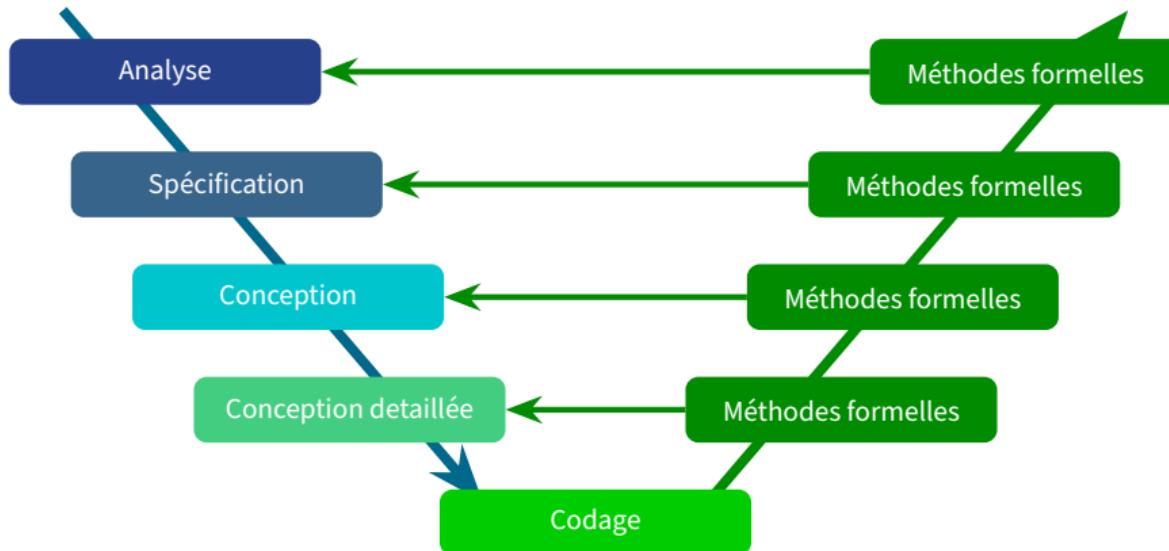


**Formal Methods for Software Engineering** ↗  
Languages, Methods, Application Domains  
Springer 2022

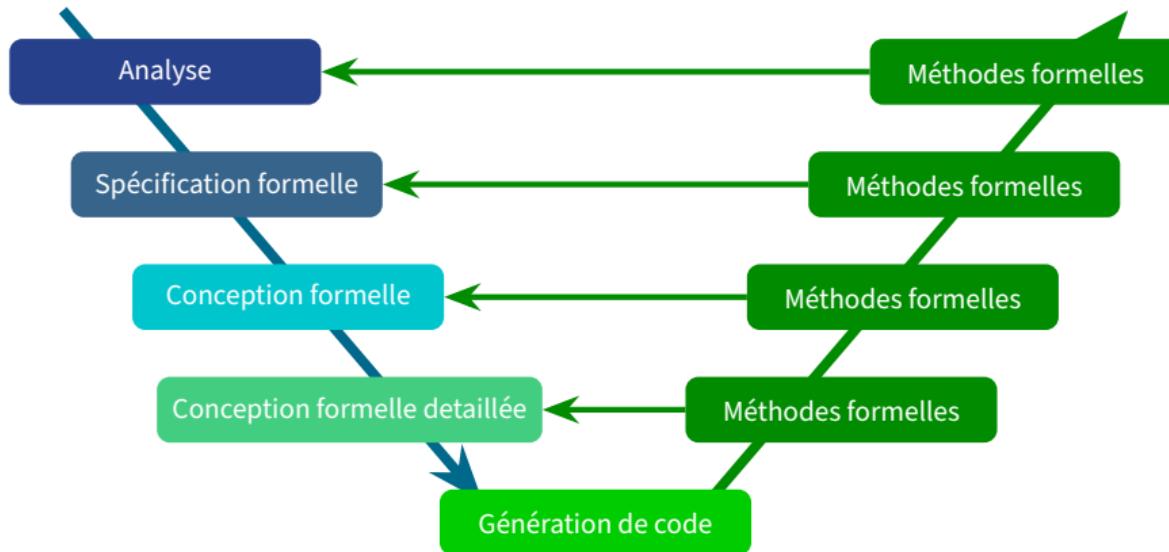
# LA PLACE DES MÉTHODES FORMELLES



# LA PLACE DES MÉTHODES FORMELLES



# LA PLACE DES MÉTHODES FORMELLES



Utiliser les méthodes formelles dans toutes les étapes.

# SPÉCIFICATION, CONCEPTION ET VÉRIFICATION

# SPÉCIFICATION, CONCEPTION ET VÉRIFICATION

- La spécification formelle → description rigoureuse et non ambiguë du comportement attendu d'un système (logiciel).

# 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)**.

# 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...).

# 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).

# 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).

# 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...).

# 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.

# 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.

# 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
-----------------	------------------	-------------------

# 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)

# 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

# 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

# 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

# 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)

# 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

# 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



# EXEMPLES DE NORMES → FERROVIAIRE

- EN 50128 Software for railway control and protection system
  - norme européenne très connue pour les logiciels critiques dans le ferroviaire



# 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)



# 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)
  - introduction des approches itératives (agile), utilisation de modèles (UML, SysML), intégration de l'IA/ML dans le cycle de développement



# 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)
  - introduction des approches itératives (agile), utilisation de modèles (UML, SysML), 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



# 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.

# EVALUATION ASSURANCE LEVEL (EAL) SELON LES CRITÈRES COMMUNS.

- **EAL1** → testé fonctionnellement (les risques sont faibles)
  - Vérifications basiques, sans grande analyse de conception.

# 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.

# 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

# 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...

# 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.

# 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.

# 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).

# 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.

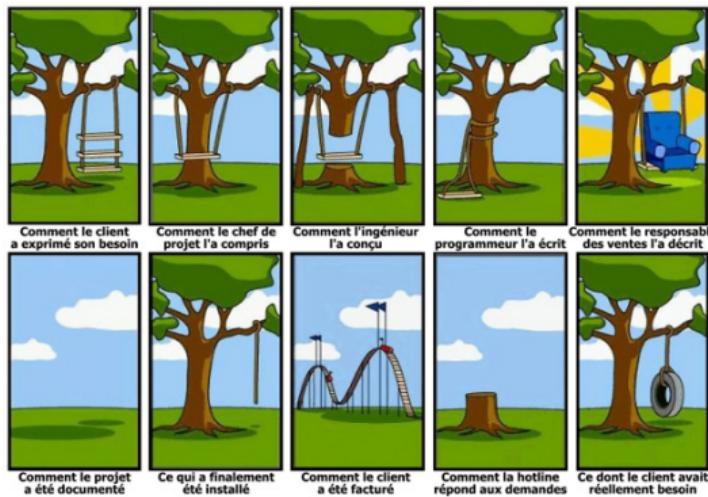
# QUELQUES MYTHES

# QUELQUES MYTHES

- L'utilisation des méthodes formelles **produit un logiciel parfait ?**

# 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

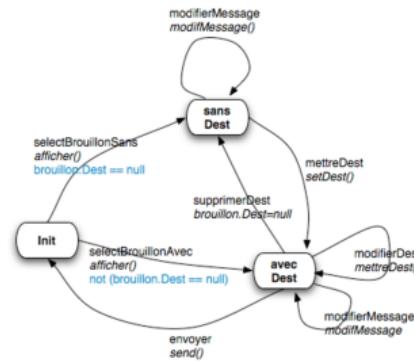


# QUELQUES MYTHES

- Utiliser les méthodes formelles  $\approx$  faire de **la preuve de programme** ?

# 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** ?

# 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** ?

# QUELQUES MYTHES

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

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

# QUELQUES MYTHES

- Les méthodes formelles augmentent les coûts de développement ?

# QUELQUES MYTHES

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

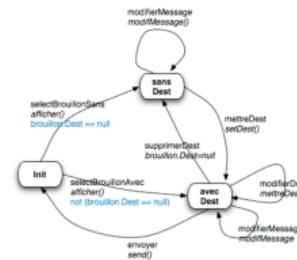


# QUELQUES MYTHES

- Les clients **ne peuvent pas comprendre** les spécifications formelles.

# 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



Systèmes complexes à logiciels prépondérants

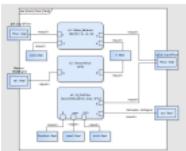
# LE CADRE DE LA ST



Systèmes complexes à logiciels prépondérants

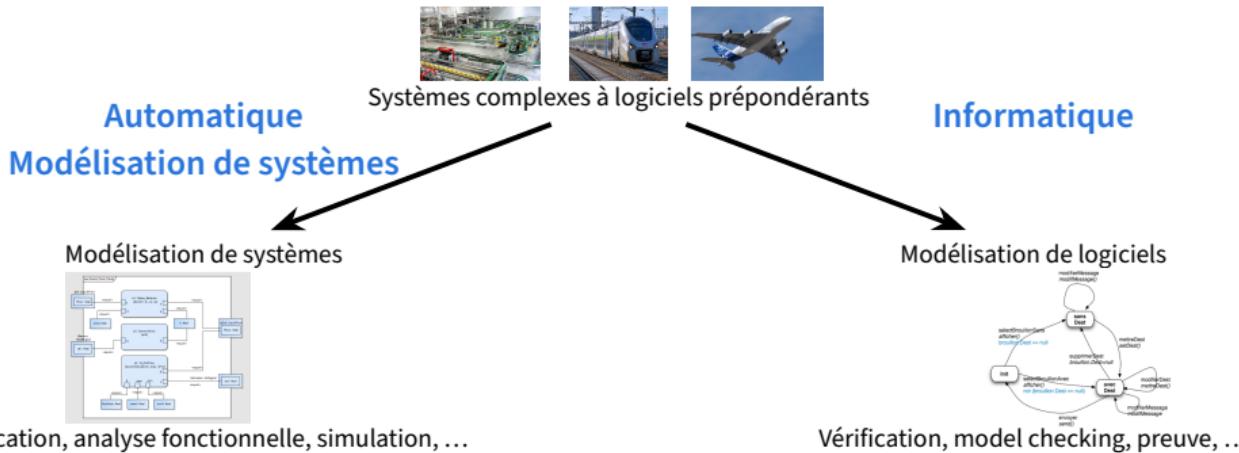
Automatique  
Modélisation de systèmes

Modélisation de systèmes

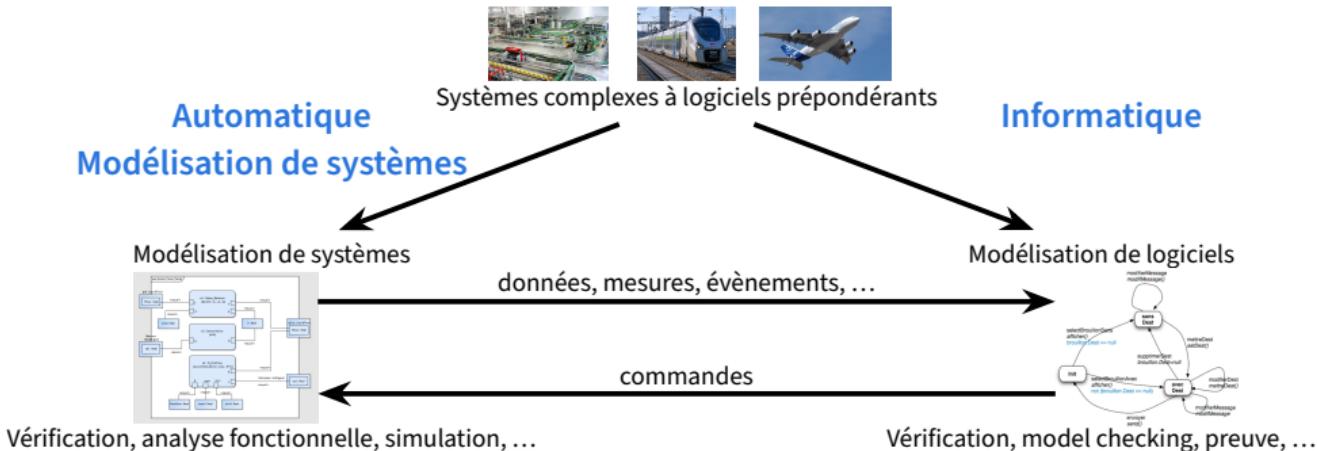


Vérification, analyse fonctionnelle, simulation, ...

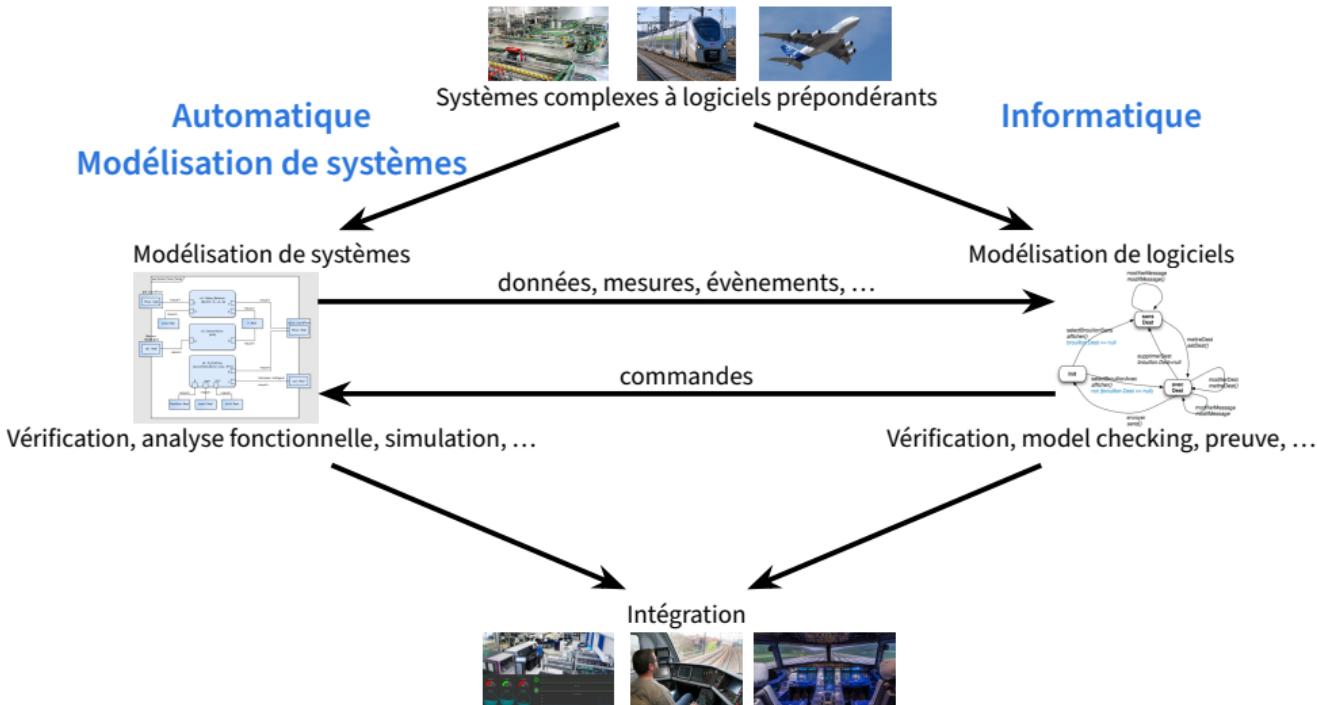
# LE CADRE DE LA ST



# LE CADRE DE LA ST

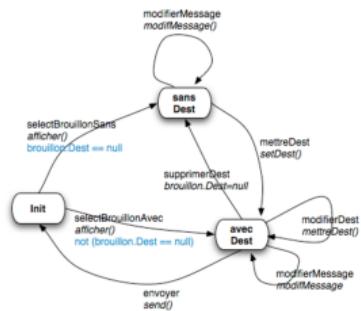


# LE CADRE DE LA ST



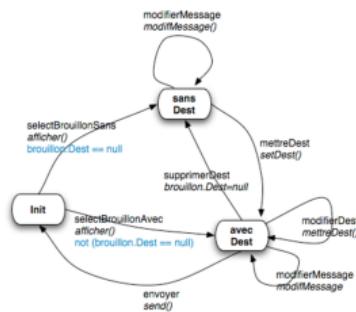
# L'OBJECTIF DE LA ST

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



# 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?



# OUTLINE

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

[Back to the begin](#) - [Back to the outline](#)

# PLANNING

Lundi 15 septembre 2025 - Amphi sa.108, Bouygues

---

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

Idir AIT-SADOUNE (CentraleSupélec)

---

**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**

---

Sayed MOHAMED-SALIH (IKOS Consulting)

# PLANNING

Mardi 23 septembre 2025 - Amphi sa.108, Bouygues

**08h15 - 09h45 Présentation des EI**

---

Idir AIT-SADOUNE (CentraleSupélec)

**10h00 - 11h30 Séminaire**

---

Émeric TOURNIAIRE (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**.

# 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”*

# 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”*

Disponibilité des résumés sur **EDUNAO** avant le **mercredi 08/10/2025 à 23h59**

# OUTLINE

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

[Back to the begin](#) - [Back to the outline](#)

# LE PROGRAMME

## CONCEPTION ET VÉRIFICATION DE SYSTÈMES CRITIQUES

**Les logiques temporelles**

Idir AIT SADOUNE (CentraleSupélec)

**3 CMs, 2 TDs (5 × 1h30)**

# 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)**

# LE PROGRAMME

## CONCEPTION ET VÉRIFICATION DE SYSTÈMES CRITIQUES

**Les logiques temporelles** Idir AIT SADOUNE (CentraleSupélec)

**3 CMs, 2 TDs** ( $5 \times 1h30$ )

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

**1 CMs, 1 TDs** ( $2 \times 1h30$ )

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

**2 CMs, 2 TDs, 1 TP** ( $6 \times 1h30$ )

# LE PROGRAMME

## CONCEPTION ET VÉRIFICATION DE SYSTÈMES CRITIQUES

**Les logiques temporelles** Idir AIT SADOUNE (CentraleSupélec)

**3 CMs, 2 TDs** ( $5 \times 1h30$ )

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

**1 CMs, 1 TDs** ( $2 \times 1h30$ )

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

**2 CMs, 2 TDs, 1 TP** ( $6 \times 1h30$ )

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

**2 CMs, 2 TDs, 1 TP** ( $6 \times 1h30$ )

# 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)

# 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 en versions PDF disponibles dans [Edunao](#).

# 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  
**en versions PDF** disponibles dans **Edunao**.
- Polycopie **en version papier** disponible.
  - disponible après sondage sur les demandes
  - contient plus d'informations que ce qui sera vu en cours.

# OUTLINE

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

[Back to the begin](#) - [Back to the outline](#)

# LES EI - ENSEIGNEMENTS D'INTÉGRATION

Présentation des sujets et des détails de l'organisation des Els  
le **mardi 23/09/2025** à **8h15**.

# OUTLINE

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

[Back to the begin](#) - [Back to the outline](#)

# VALIDATION DE LA ST

- La **ST5** valide une Unité d'Enseignement (**UE**) **Séquence Thématique** dédiée à **la modélisation fonctionnelle et la régulation**.

# 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.

# 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.

# 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.

# 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.

# 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.**

# 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

# 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

- **Le 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

# 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

- **Le 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

- **L'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

# ORGANISATION DES RATTRAPAGES

- **Modules 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.

# ORGANISATION DES RATTRAPAGES

- **Modules 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

# ORGANISATION DES RATTRAPAGES

- **Modules 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.

# OUTLINE

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

[Back to the begin](#) - [Back to the outline](#)

# 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) ↗

# THANK YOU

[Back to the begin](#) - [Back to the outline](#)