Spécification, Construction et Vérification de programmes

Le parcours d'une pensée scientifique sur une quarantaine d'années

Jean-Raymond Abrial

Séminaire au Collège de France

1er Avril 2015

- Bonjour à tous

Préambule

- Bonjour à tous

- Et merci à Gérard Berry de son invitation pour ce séminaire

Préambule

- Bonjour à tous

- Et merci à Gérard Berry de son invitation pour ce séminaire

- En fait, je suis très ému d'être de ce côté-ci de l'amphithéatre

- Bonjour à tous

- Et merci à Gérard Berry de son invitation pour ce séminaire

- En fait, je suis très ému d'être de ce côté-ci de l'amphithéatre

- Car, il y a 40 ans, je n'aurais jamais imaginé être là

- Bonjour à tous

- Et merci à Gérard Berry de son invitation pour ce séminaire

- En fait, je suis très ému d'être de ce côté-ci de l'amphithéatre

- Car, il y a 40 ans, je n'aurais jamais imaginé être là

- En effet, je venais écouter ici même ...

Roland Barthes

Roland Barthes

- Dont on fête cette année le centième anniversaire de la naissance

- Roland Barthes inaugurait la nouvelle chaire de Sémiologie

- Roland Barthes inaugurait la nouvelle chaire de Sémiologie

- Par un cours passionnant dont le titre était ...

- Roland Barthes inaugurait la nouvelle chaire de Sémiologie

- Par un cours passionnant dont le titre était ...

- Toute proportion gardée, bien entendu

- Toute proportion gardée, bien entendu

- Serions-nous capable de vivre avec cette technologie?

Vivre Ensemble

- Toute proportion gardée, bien entendu

- Serions-nous capable de vivre avec cette technologie?

- Cette informatique si envahissante mais aussi si fragile

- Toute proportion gardée, bien entendu

- Serions-nous capable de vivre avec cette technologie?

- Cette informatique si envahissante mais aussi si fragile

- Pour tenter de répondre à cette question

  (à laquelle Gérard Berry répond déjà si brillamment)

- Toute proportion gardée, bien entendu

- Serions-nous capable de vivre avec cette technologie?

- Cette informatique si envahissante mais aussi si fragile

- Pour tenter de répondre à cette question
  (à laquelle Gérard Berry répond déjà si brillamment)

- Je voudrais témoigner de mon parcours scientifique
  qui s'étend sur une quarantaine d'années

- Il y a deux catégories de chercheurs:

- Il y a deux catégories de chercheurs:
    - les grands, éclectiques: ils touchent à de nombreux domaines

- Il y a deux catégories de chercheurs:
    - les grands, éclectiques: ils touchent à de nombreux domaines
    - les petits, monomaniaques: ils font toujours la même chose

- Il y a deux catégories de chercheurs:
    - les grands, éclectiques: ils touchent à de nombreux domaines
    - les petits, monomaniaques: ils font toujours la même chose

- Je fais partie de la seconde catégorie

- Il y a deux catégories de chercheurs:
    - les grands, éclectiques: ils touchent à de nombreux domaines
    - les petits, monomaniaques: ils font toujours la même chose

- Je fais partie de la seconde catégorie

- En fait, j'ai passé 40 ans à faire la même chose

Qu’ai-je fait?

Qu'ai-je fait? Réponse:

- Comment savoir si ce qu'on programme est bien ce qu'on voulait?

Qu'ai-je fait? Réponse:

- Comment savoir si ce qu'on programme est bien ce qu'on voulait?

- Éviter "une mauvaise adéquation entre la tâche qu'on assigne à la machine et celle qu'on veut qu'elle remplisse en réalité" (Stuart Russell)

Qu'ai-je fait? Réponse:

- Comment savoir si ce qu'on programme est bien ce qu'on voulait?

- Éviter "une mauvaise adéquation entre la tâche qu'on assigne à la machine et celle qu'on veut qu'elle remplisse en réalité" (Stuart Russell)

- Et par la même occasion: BIEN SAVOIR CE QUE L'ON VEUT

Qu'ai-je fait? Réponse:

- Comment savoir si ce qu'on programme est bien ce qu'on voulait?

- Éviter "une mauvaise adéquation entre la tâche qu'on assigne à la machine et celle qu'on veut qu'elle remplisse en réalité" (Stuart Russell)

- Et par la même occasion: BIEN SAVOIR CE QUE L'ON VEUT

- Pour cela, j'ai développé (avec d'autres): Z, B et enfin Event-B

Qu'ai-je fait? Réponse:

- Comment savoir si ce qu'on programme est bien ce qu'on voulait?

- Éviter "une mauvaise adéquation entre la tâche qu'on assigne à la machine et celle qu'on veut qu'elle remplisse en réalité" (Stuart Russell)

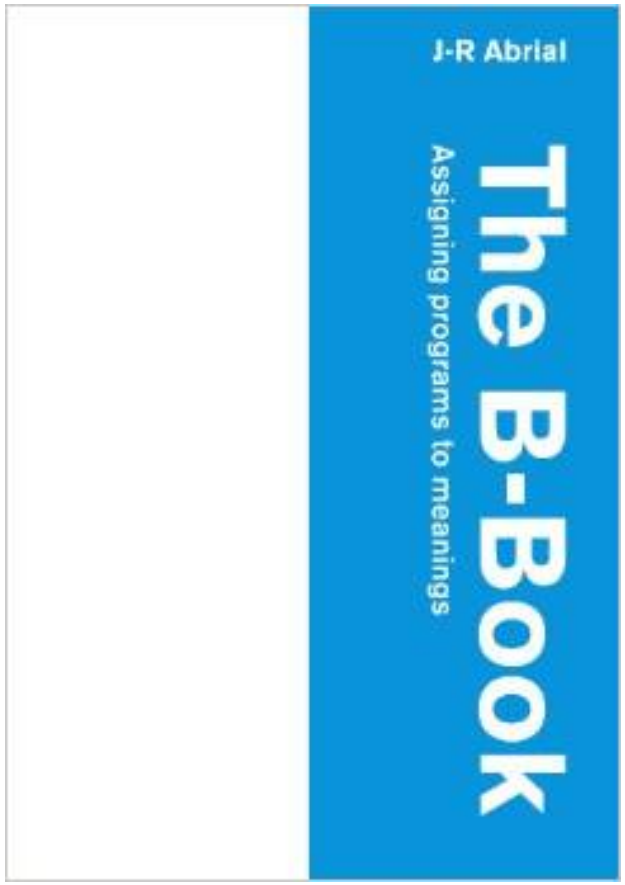
- Et par la même occasion: BIEN SAVOIR CE QUE L'ON VEUT

- Pour cela, j'ai développé (avec d'autres): Z, B et enfin Event-B

- Au cours de ce séminaire, je voudrais témoigner de cette évolution

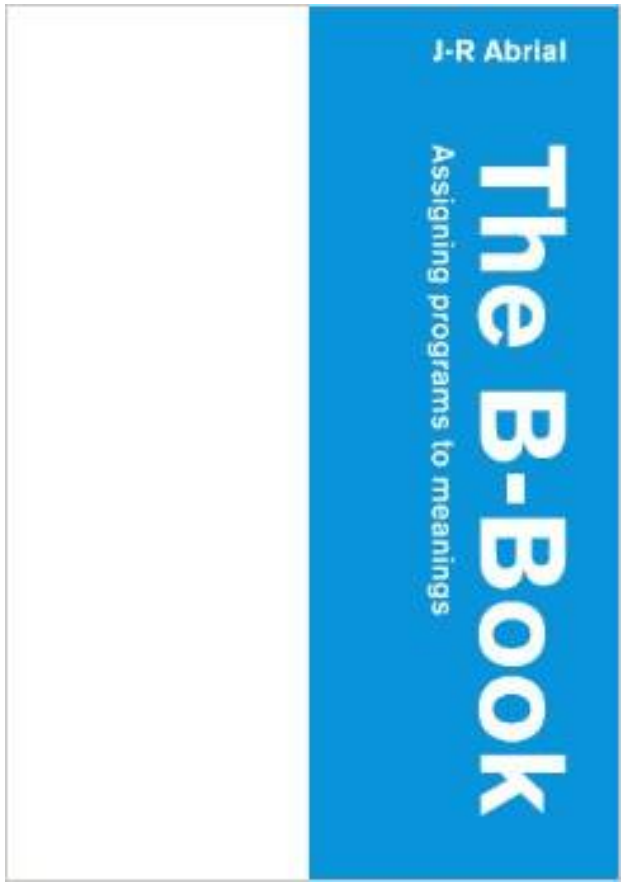
- Z: J.-R. Abrial, S.A. Schuman, B. Meyer. *Specification Language*. On the Construction of Programs (1980)

- Z: J.-R. Abrial, S.A. Schuman, B. Meyer. *Specification Language*. On the Construction of Programs (1980)

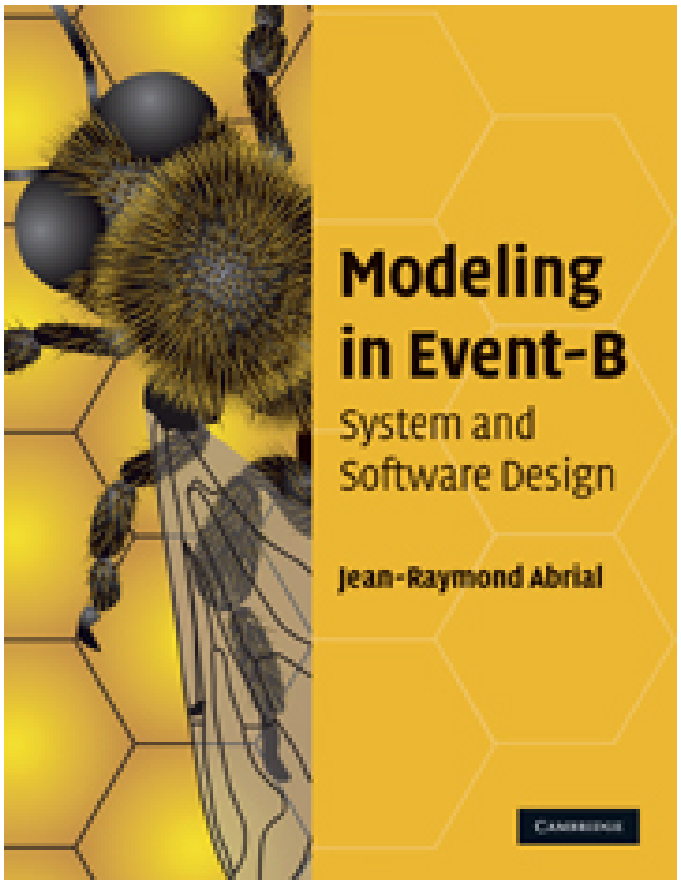


1996

- Z: J.-R. Abrial, S.A. Schuman, B. Meyer. *Specification Language*. On the Construction of Programs (1980)



1996



2010

Plan de cette Présentation

- Historique d'une lente evolution:

Plan de cette Présentation

- Historique d'une lente evolution:
    - Au début, je vais raconter des histoires

Plan de cette Présentation

- Historique d'une lente evolution:
  - Au début, je vais raconter des histoires
  - À la fin, mon exposé sera un tout petit peu plus technique avec un exemple

Plan de cette Présentation

- Historique d'une lente evolution:
  - Au début, je vais raconter des histoires
  - À la fin, mon exposé sera un tout petit peu plus technique avec un exemple
- Conclusion et suggestions

- J'ai fait partie de l'équipe **Green** (l'ancêtre du langage ADA)

  dirigée par Jean Ichbiah

- J'ai fait partie de l'équipe **Green** (l'ancêtre du langage ADA) dirigée par Jean Ichbiah

- J'ai écrit des "programmes" en **Green**

Comment tout a commencé: Green

- J'ai fait partie de l'équipe **Green** (l'ancêtre du langage ADA) dirigée par Jean Ichbiah

- J'ai écrit des "programmes" en **Green**

- Mais comment savoir si ces programmes étaient corrects?

Comment tout a commencé: Green

- J'ai fait partie de l'équipe **Green** (l'ancêtre du langage ADA) dirigée par Jean Ichbiah

- J'ai écrit des "programmes" en **Green**

- Mais comment savoir si ces programmes étaient corrects?

- S'ils faisaient bien ce que je voulais qu'ils fassent

Comment tout a commencé: Green

- J'ai fait partie de l'équipe **Green** (l'ancêtre du langage ADA) dirigée par Jean Ichbiah

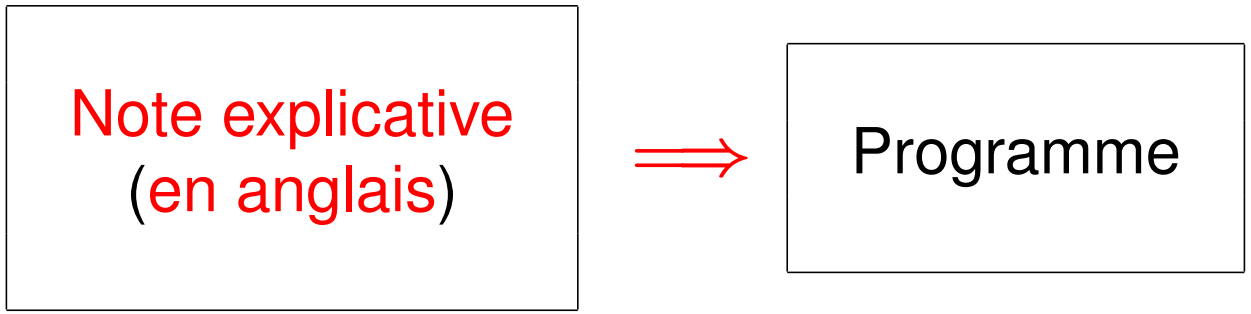
- J'ai écrit des "programmes" en **Green**

- Mais comment savoir si ces programmes étaient corrects?

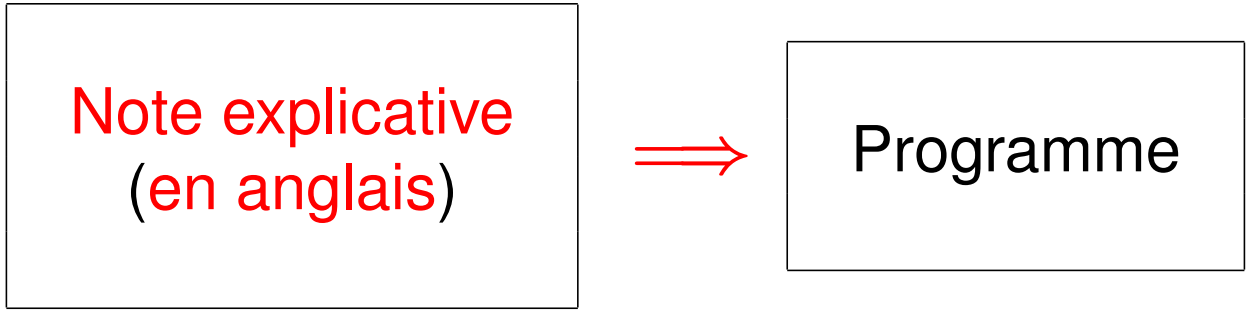
- S'ils faisaient bien ce que je voulais qu'ils fassent

- J'ai écrit pour cela des petites notes (en anglais) pour expliquer

Illustration

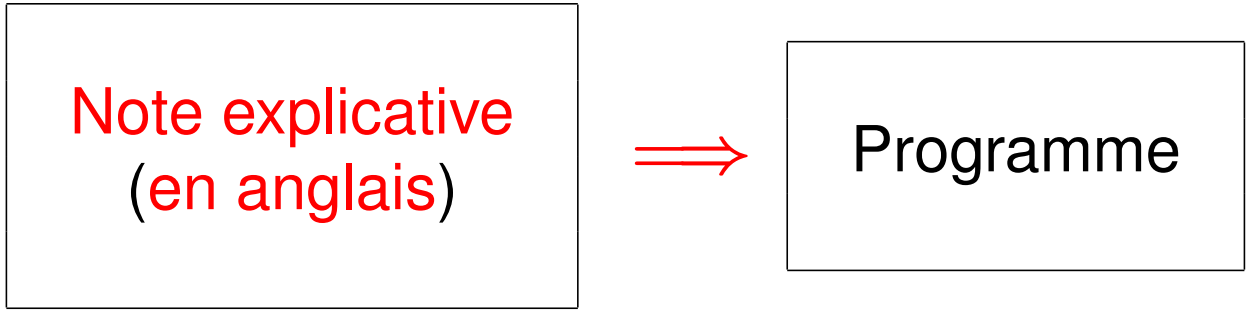


Illustration



- J’avais bien écrit des notes explicatives

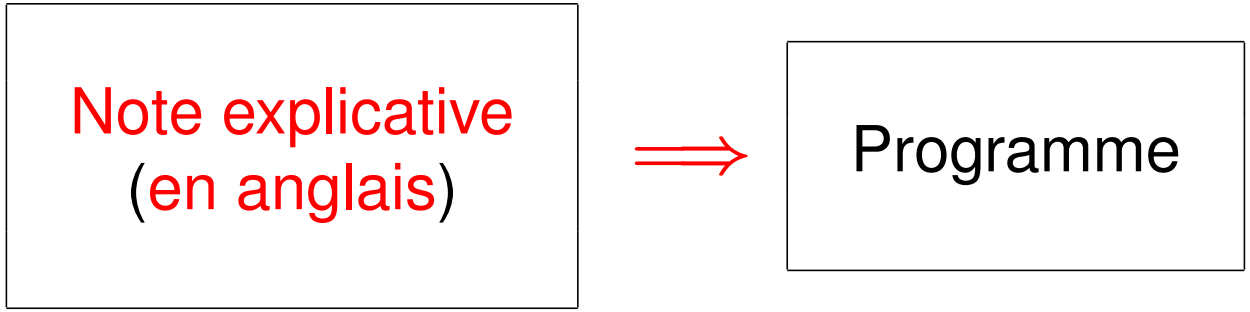
Illustration



- J'avais bien écrit des notes explicatives

- Mais le programme correspondait-il aux notes explicatives?

Illustration

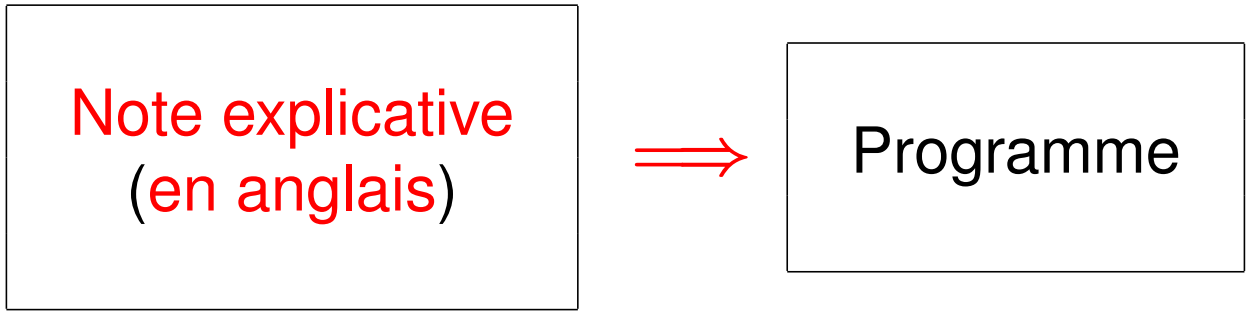


- J'avais bien écrit des notes explicatives

- Mais le programme correspondait-il aux notes explicatives?

- En fait, j'avais simplement repoussé le problème

Illustration



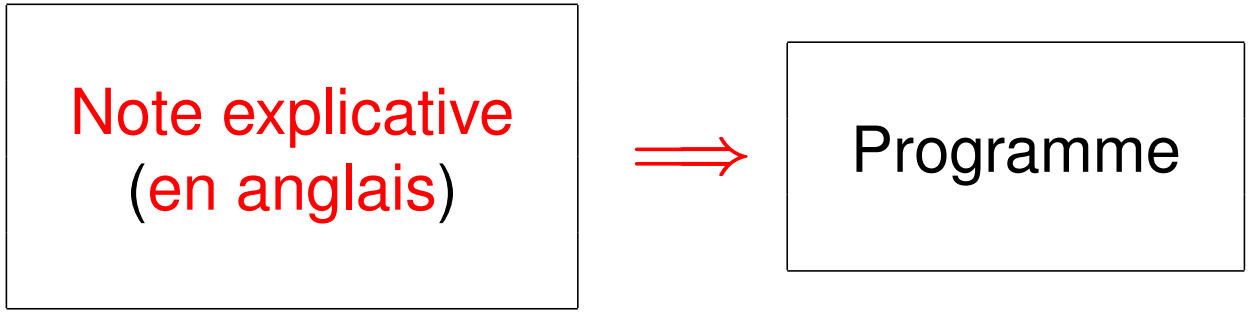
- J'avais bien écrit des notes explicatives

- Mais le programme correspondait-il aux notes explicatives?

- En fait, j'avais simplement repoussé le problème

- Car, comment comparer de l'anglais à un programme?

Illustration



- J'avais bien écrit des notes explicatives

- Mais le programme correspondait-il aux notes explicatives?

- En fait, j'avais simplement repoussé le problème

- Car, comment comparer de l'anglais à un programme?

- Je voulais un moyen systématique pour faire cette comparaison

Recherche d'une Notation

- Est-il possible de remplacer l'anglais par une notation formelle?

Recherche d'une Notation

- Est-il possible de remplacer l'anglais par une notation formelle?

- À ce moment-là, je lisais "Théorie des Ensembles" de Bourbaki

Recherche d'une Notation

- Est-il possible de remplacer l'anglais par une notation formelle?

- À ce moment-là, je lisais "Théorie des Ensembles" de Bourbaki

- J'avais mis très longtemps à lire juste les 50 premières pages

Recherche d'une Notation

- Est-il possible de remplacer l'anglais par une notation formelle?

- À ce moment-là, je lisais "Théorie des Ensembles" de Bourbaki

- J'avais mis très longtemps à lire juste les 50 premières pages

- Intéressé de voir comment la théorie des ensembles était utilisée

- Le bon usage des mathématiques:

- Le bon usage des mathématiques:
    - Expressions rigoureuses (pas d'ambiguités).

- Le bon usage des mathématiques:
    - Expressions rigoureuses (pas d'ambiguités).
    - L'écriture de preuves

Preuves

- Le bon usage des mathématiques:
    - Expressions rigoureuses (pas d'ambiguités).
    - L'écriture de preuves

- Je me proposais d'utiliser la notation de la théorie des ensembles

Preuves

- Le bon usage des mathématiques:
    - Expressions rigoureuses (pas d'ambiguités).
    - L'écriture de preuves

- Je me proposais d'utiliser la notation de la théorie des ensembles

- Et de faire des preuves comme moyen de comparaison (???)

Preuves

- Le bon usage des mathématiques:
    - Expressions rigoureuses (pas d'ambiguités).
    - L'écriture de preuves

- Je me proposais d'utiliser la notation de la théorie des ensembles

- Et de faire des preuves comme moyen de comparaison (???)

- Tout ceci était encore très vague dans ma tête

Certains Informaticiens n'aimaient pas ça du tout (1)

- On m'avait demandé de faire un cours dans une École d'été

Certains Informaticiens n'aimaient pas ça du tout (1)

- On m'avait demandé de faire un cours dans une École d'été

- Je proposais un exposé autour de l'approche que je viens de décrire

Certains Informaticiens n'aimaient pas ça du tout (1)

- On m'avait demandé de faire un cours dans une École d'été

- Je proposais un exposé autour de l'approche que je viens de décrire

- Ma participation à cette École d'été a été immédiatement annulée

Certains Informaticiens n'aimaient pas ça du tout (1)

- On m'avait demandé de faire un cours dans une École d'été

- Je proposais un exposé autour de l'approche que je viens de décrire

- Ma participation à cette École d'été a été immédiatement annulée

- Raison: aucun intérêt pour ce genre de sujet

Certains Informaticiens n'aimaient pas ça du tout (1)

- On m'avait demandé de faire un cours dans une École d'été

- Je proposais un exposé autour de l'approche que je viens de décrire

- Ma participation à cette École d'été a été immédiatement annulée

- Raison: aucun intérêt pour ce genre de sujet

- Les informaticiens n'aiment pas la théorie de ensembles

Certains n'aimaient pas ça du tout (2)

- Les informaticiens confondent Mathématiques et Informatique

Certains n'aimaient pas ça du tout (2)

- Les informaticiens confondent Mathématiques et Informatique

- Ils confondent prédicats and expressions booléennes

Certains n'aimaient pas ça du tout (2)

- Les informaticiens confondent Mathématiques et Informatique

- Ils confondent prédicats and expressions booléennes

- Les mathématiciens, eux, n'aiment pas beaucoup la logique

Certains n'aimaient pas ça du tout (2)

- Les informaticiens confondent Mathématiques et Informatique

- Ils confondent prédicats and expressions booléennes

- Les mathématiciens, eux, n'aiment pas beaucoup la logique

- Difficile de réconcilier les deux communautés

Certains n'aimaient pas ça du tout (2)

- Les informaticiens confondent Mathématiques et Informatique

- Ils confondent prédicats and expressions booléennes

- Les mathématiciens, eux, n'aiment pas beaucoup la logique

- Difficile de réconcilier les deux communautés

- Heureusement, j'ai eu de la chance, car ...

- À la fin des années 70, j'ai été invité par Tony Hoare à Oxford

Oxford: Z

- À la fin des années 70, j'ai été invité par Tony Hoare à Oxford

- Travail commun avec Bernard Sufrin, Tim Clement, Ib Sørensen

- À la fin des années 70, j'ai été invité par Tony Hoare à Oxford

- Travail commun avec Bernard Sufrin, Tim Clement, Ib Sørensen

- Développement d'une notation basée sur la théorie des ensembles

Oxford: Z

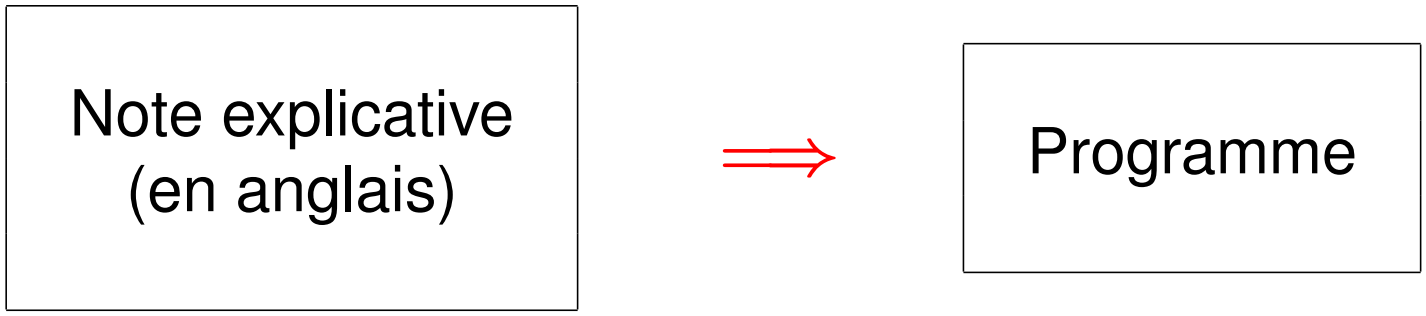
- À la fin des années 70, j'ai été invité par Tony Hoare à Oxford

- Travail commun avec Bernard Sufrin, Tim Clement, Ib Sørensen

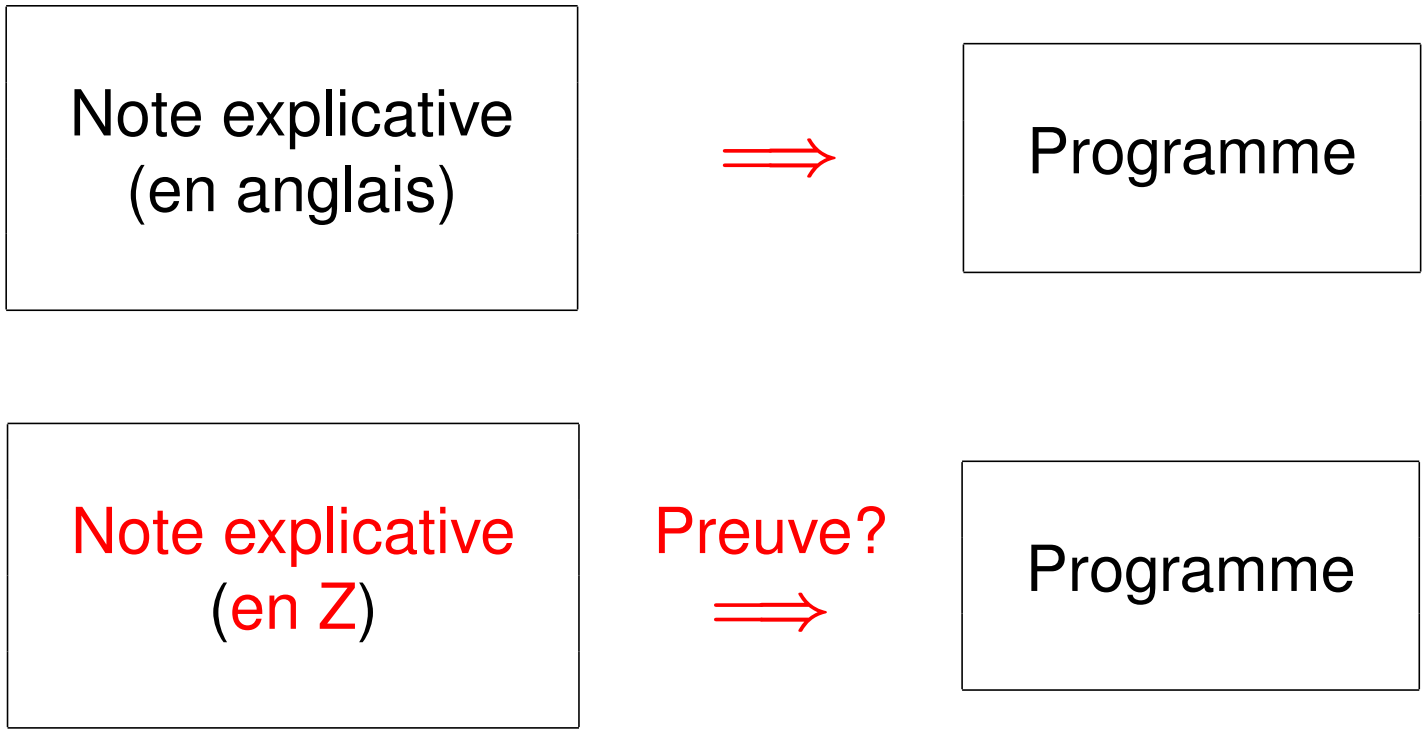
- Développement d'une notation basée sur la théorie des ensembles

- Z ÉTAIT NÉ (fin des années 70)

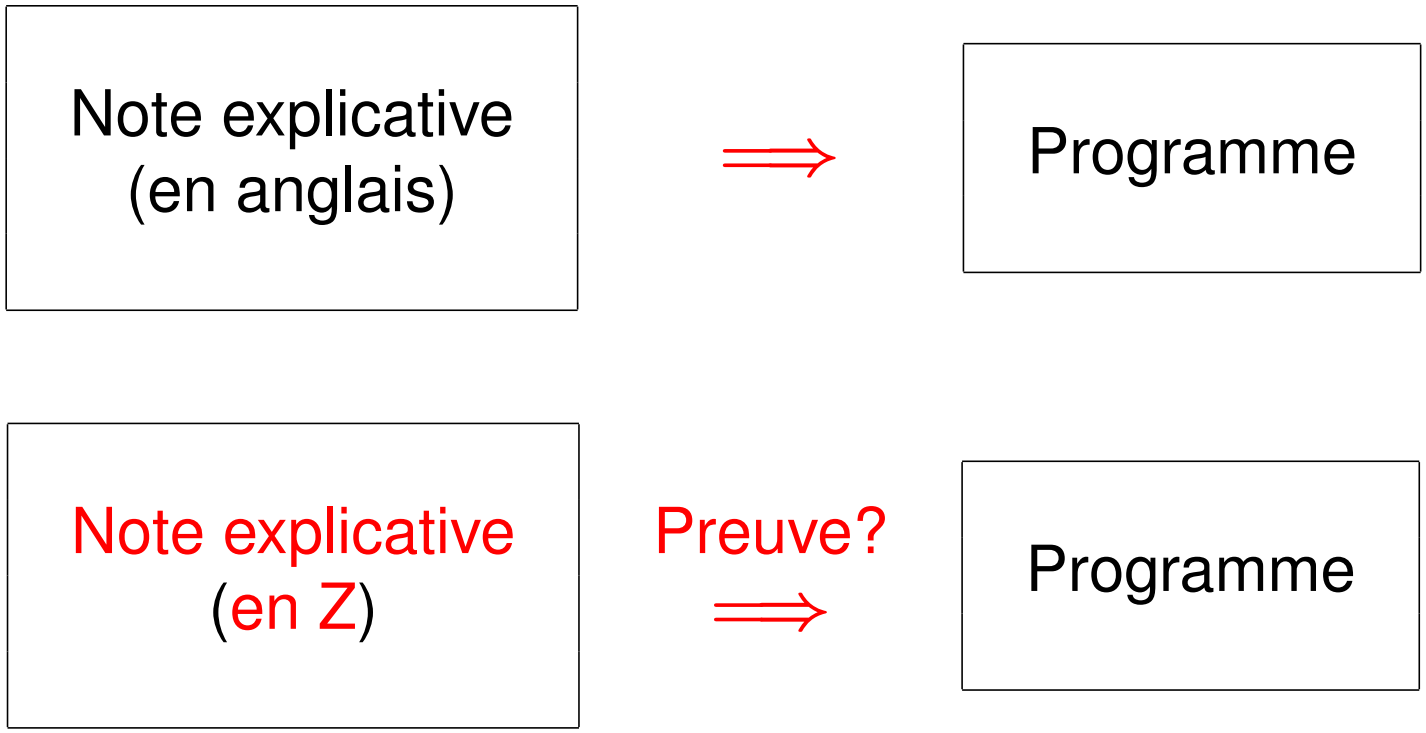
Évolution: un Progrès ... Apparent



Évolution: un Progrès ... Apparent

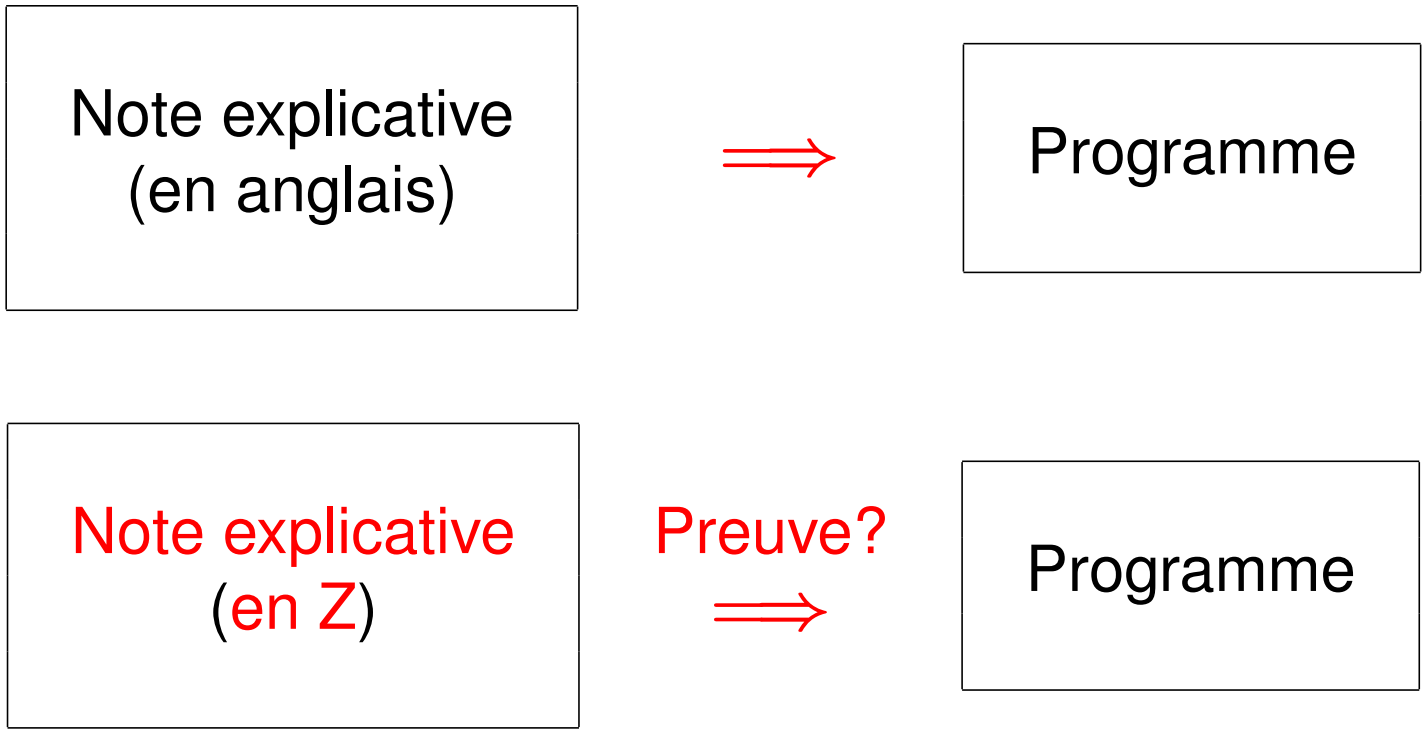


Évolution: un Progrès ... Apparent



- Mais on était loin de résoudre le problème initial: la comparaison des notes (maintenant formalisées en Z) et des programmes

Évolution: un Progrès ... Apparent



- Mais on était loin de résoudre le problème initial: la comparaison des notes (maintenant formalisées en Z) et des programmes

- Quelles preuves pouvaient tenir lieu de comparaison?

- Au début des années 80, je suis rentré en France

Aller plus loin: B

- Au début des années 80, je suis rentré en France

- Quelques orientations nouvelles:

- Au début des années 80, je suis rentré en France

- Quelques orientations nouvelles:
    - Simplifier Z

- Au début des années 80, je suis rentré en France

- Quelques orientations nouvelles:
    - Simplifier Z
    - Structurer Z

Aller plus loin: B

- Au début des années 80, je suis rentré en France

- Quelques orientations nouvelles:
  - Simplifier Z
  - Structurer Z
  - Introduire le raffinement (Back, Hoare, Morgan, Jones, ...)

Aller plus loin: B

- Au début des années 80, je suis rentré en France

- Quelques orientations nouvelles:
  - Simplifier Z
  - Structurer Z
  - Introduire le raffinement (Back, Hoare, Morgan, Jones, ...)
  - Automatiser la programmation

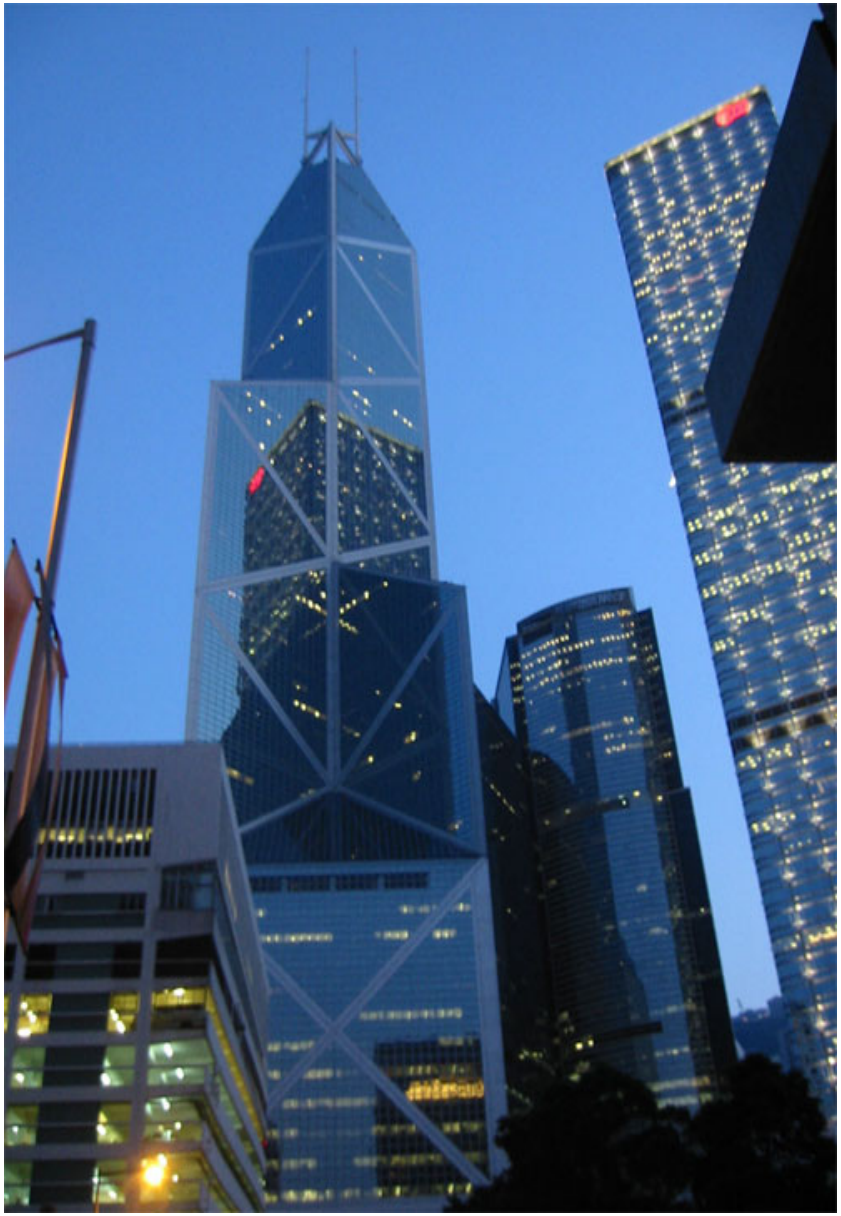
- Au début des années 80, je suis rentré en France

- Quelques orientations nouvelles:
  - Simplifier Z
  - Structurer Z
  - Introduire le raffinement (Back, Hoare, Morgan, Jones, ...)
  - Automatiser la programmation

- B ÉTAIT NÉ (fin des années 80)

Un Petit Détour par d'Autres Disciplines: Aviation

Un Petit Détour par d'Autres Disciplines: Architecture



Un Petit Détour par d'Autres Disciplines: Génie Civil

- Existe-t-il des approaches similaires dans d'autres disciplines?

- Existe-t-il des approaches similaires dans d'autres disciplines?

- Consistant à faire quelquechose AVANT la construction proprement dite

- Existe-t-il des approaches similaires dans d'autres disciplines?

- Consistant à faire quelquechose AVANT la construction proprement dite

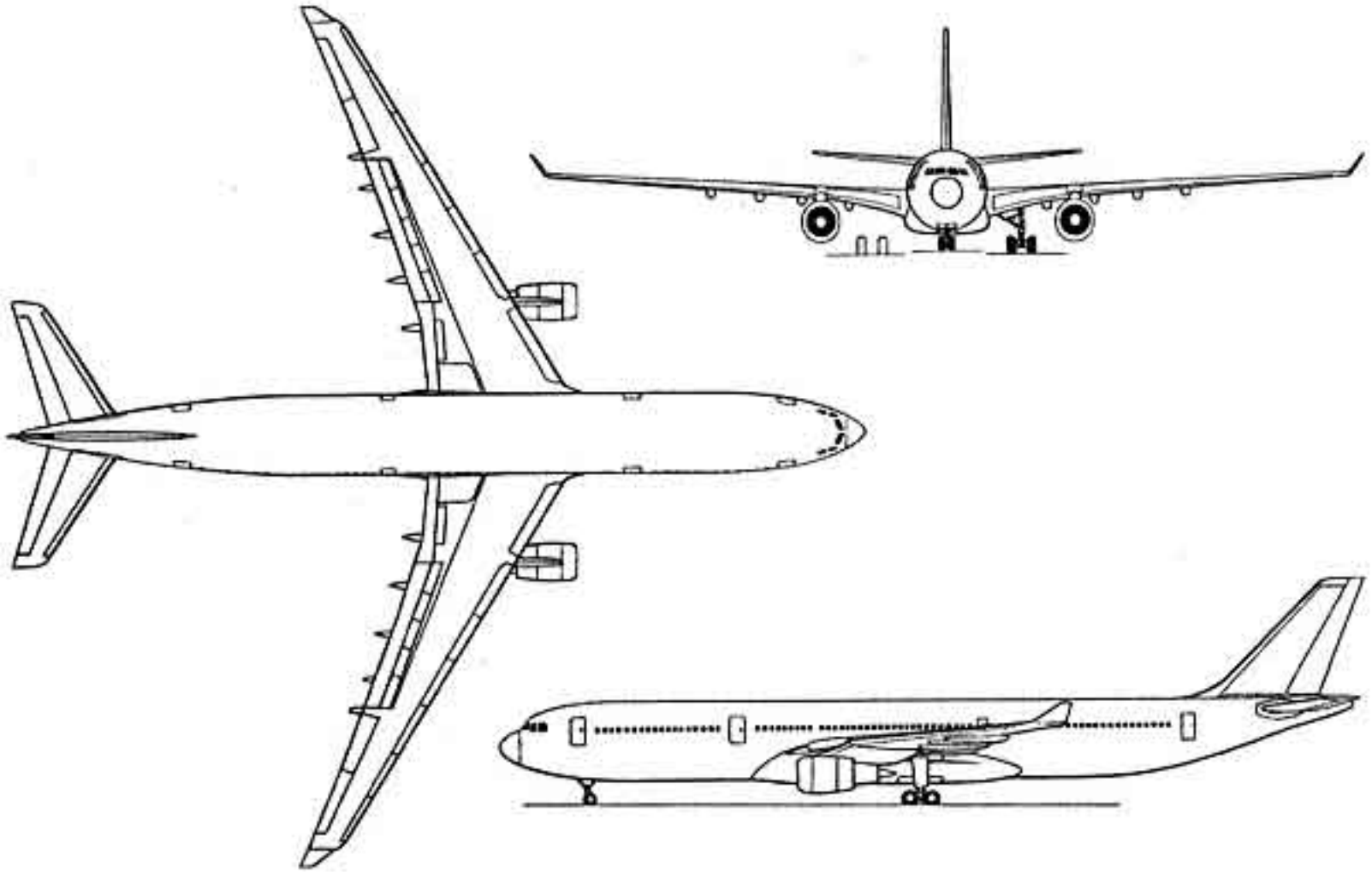
- OUI

- Existe-t-il des approaches similaires dans d'autres disciplines?

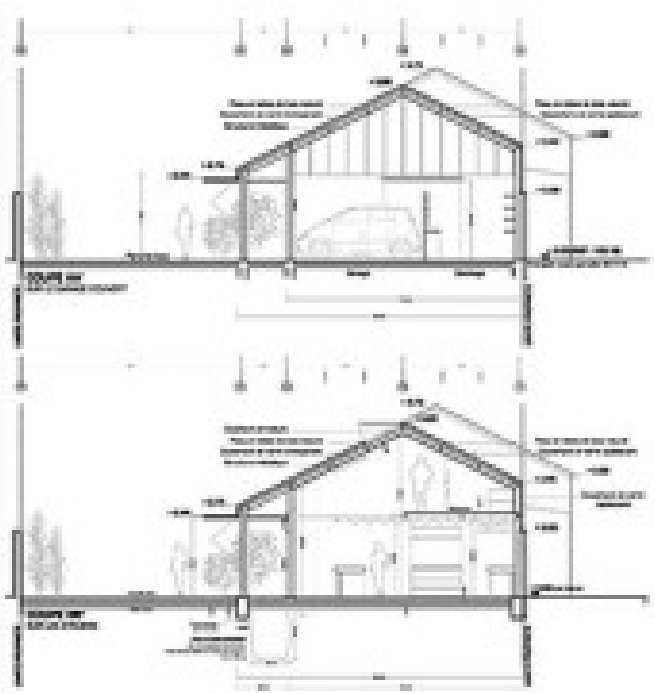
- Consistant à faire quelquechose AVANT la construction proprement dite

- OUI, les dessins industriels et les plans

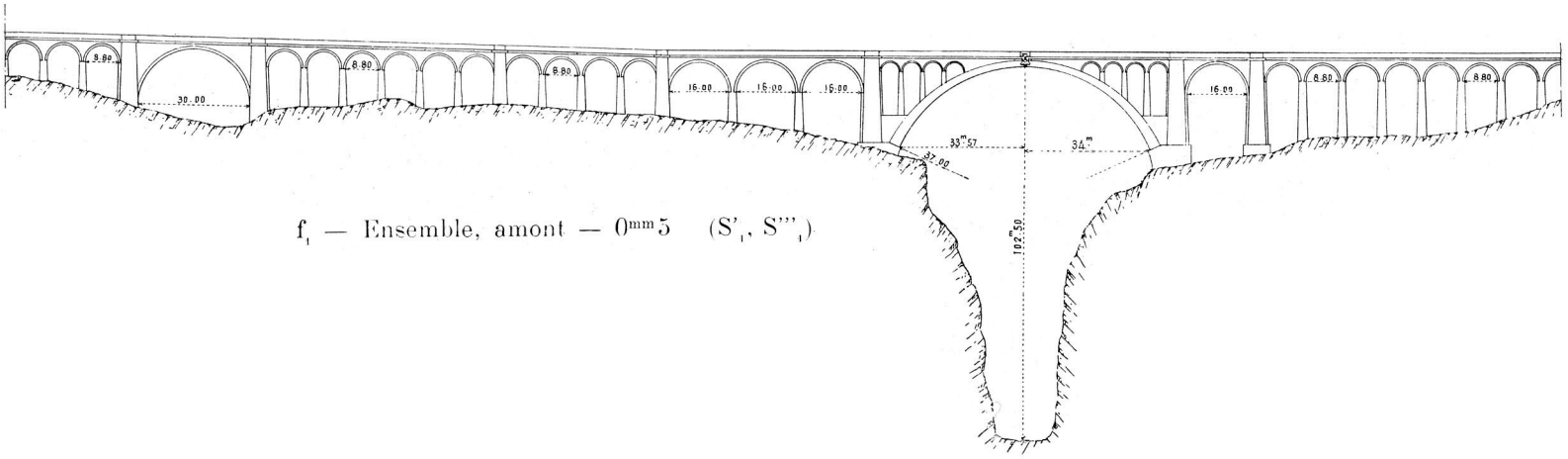
Les Dessins Industriels: Avions



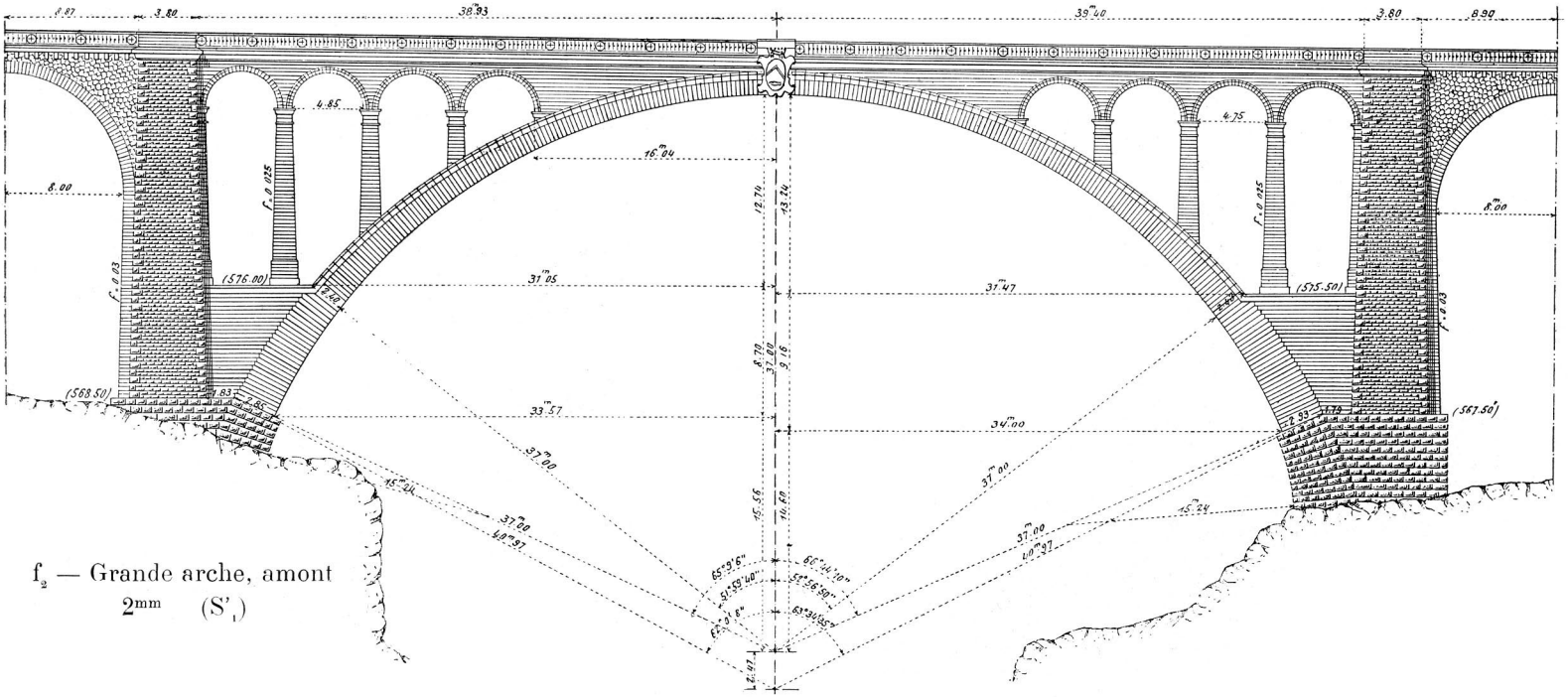
Les Dessins Industriels: Architecture



Les Dessins industriels: Ponts

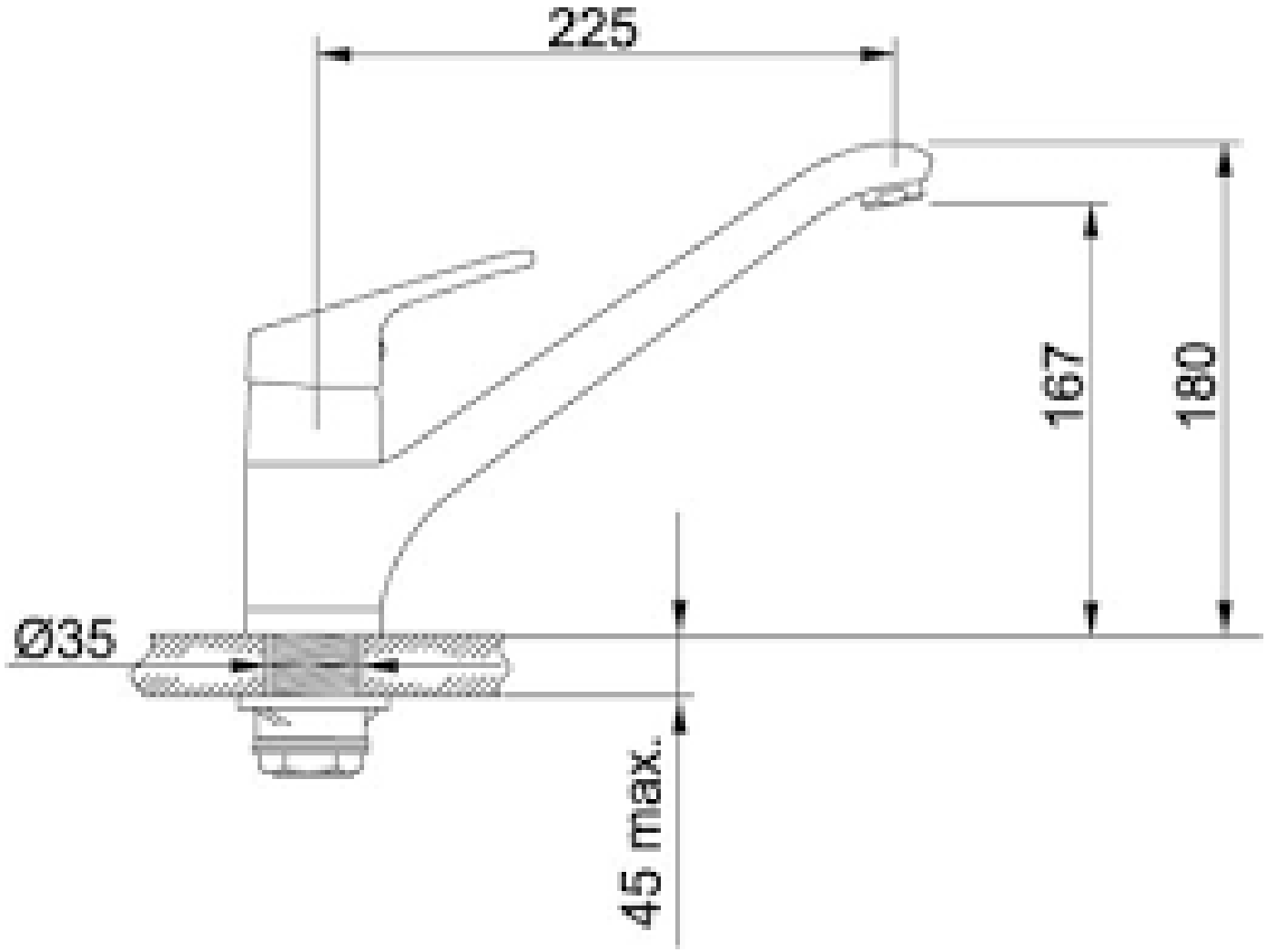


f_1 — Ensemble, amont — $0^{mm}5$ (S'_1, S'''_1)



f_2 — Grande arche, amont
2^{mm} (S'_1)

Les Dessins Industriels: Même un Robinet!



Avant-Après

Études très nombreuses

Avion

Essais ... Certification

Pas grand chose

Programme

Tests ...

Après pour un Programme

- Tests et corrections

- Assertions (Floyd, Hoare, Dijkstra, ...)

- Interprétation abstraite (Cousot)

- Model checking

- Preuve

- Rien ou UML

- Mon but: Faire beaucoup plus dans ce domaine

- Mais, revenons pour un moment sur les dessins industriels

Un Dessin Industriel, qu'est-ce que c'est?

Un Dessin Industriel, qu'est-ce que c'est?

- Une certaine representation de ce que l'on veut construire

Un Dessin Industriel, qu'est-ce que c'est?

- Une certaine representation de ce que l'on veut construire

- Mais cette représentation n'est pas une maquette

Un Dessin Industriel, qu'est-ce que c'est?

- Une certaine representation de ce que l'on veut construire

- Mais cette représentation n'est pas une maquette

- La base manque: on ne peut pas "conduire" le dessin d'une voiture

Un Dessin Industriel, qu'est-ce que c'est?

- Une certaine representation de ce que l'on veut construire

- Mais cette représentation n'est pas une maquette

- La base manque: on ne peut pas "conduire" le dessin d'une voiture

- Mais on peut raisonner sur notre futur système durant sa conception

Un Dessin Industriel, qu'est-ce que c'est?

- Une certaine representation de ce que l'on veut construire

- Mais cette représentation n'est pas une maquette

- La base manque: on ne peut pas "conduire" le dessin d'une voiture

- Mais on peut raisonner sur notre futur système durant sa conception

- Est-ce important? (d'après les experts)

Un Dessin Industriel, qu'est-ce que c'est?

- Une certaine représentation de ce que l'on veut construire

- Mais cette représentation n'est pas une maquette

- La base manque: on ne peut pas "conduire" le dessin d'une voiture

- Mais on peut raisonner sur notre futur système durant sa conception

- Est-ce important? (d'après les experts) OUI

- Définir et calculer le fonctionnement du système (ce qu'il doit faire)

- Définir et calculer le fonctionnement du système (ce qu'il doit faire)

- Incorporer les contraintes du système (ce qu'il ne doit pas faire)

- Définir et calculer le fonctionnement du système (ce qu'il doit faire)

- Incorporer les contraintes du système (ce qu'il ne doit pas faire)

- En définir l'architecture

- Définir et calculer le fonctionnement du système (ce qu'il doit faire)

- Incorporer les contraintes du système (ce qu'il ne doit pas faire)

- En définir l'architecture

- Tout ceci est basé sur des théories scientifiques bien établies
    - résistance des matériaux,
    - mécanique des fluides,
    - gravitation,
    - etc.

- Utiliser des conventions pré-définies

- Utiliser des conventions pré-définies

- Ces conventions doivent faciliter raisonnements et communication

- Utiliser des conventions pré-définies

- Ces conventions doivent faciliter raisonnements et communication

- Ajouter des détails sur des versions plus précises de nos plans

- Utiliser des conventions pré-définies

- Ces conventions doivent faciliter raisonnements et communication

- Ajouter des détails sur des versions plus précises de nos plans

- Repousser des choix en élaborant des options

- Utiliser des conventions pré-définies

- Ces conventions doivent faciliter raisonnements et communication

- Ajouter des détails sur des versions plus précises de nos plans

- Repousser des choix en élaborant des options

- Décomposer un plan en plusieurs sous-plans

- Utiliser des conventions pré-définies

- Ces conventions doivent faciliter raisonnements et communication

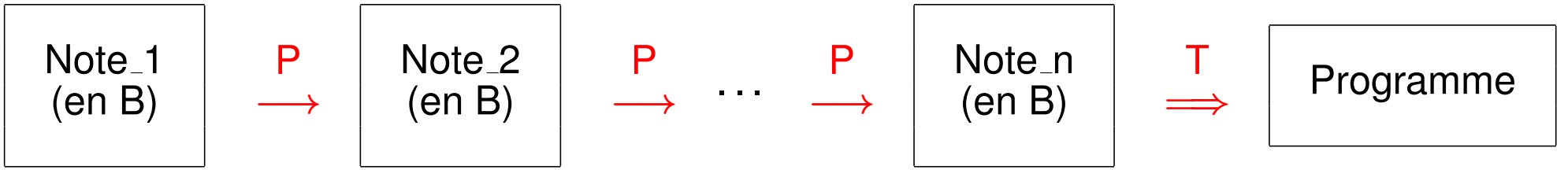
- Ajouter des détails sur des versions plus précises de nos plans

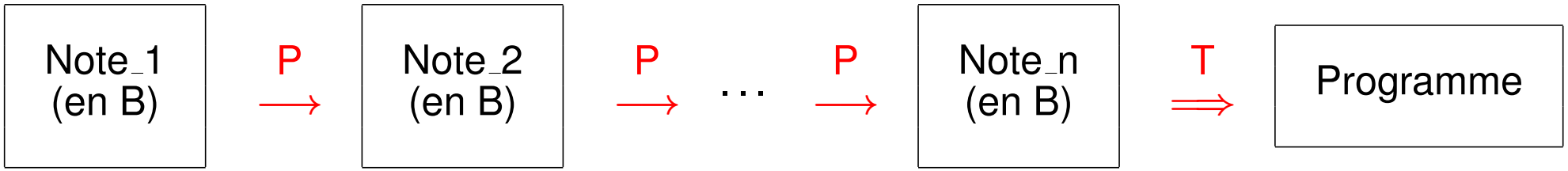
- Repousser des choix en élaborant des options

- Décomposer un plan en plusieurs sous-plans

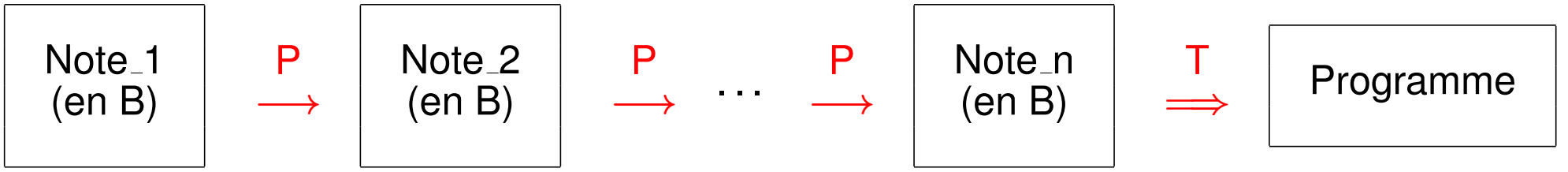
- Réutiliser de “vieux” plans avec quelques changements

Explications simplifiée de B: Faire des Plans





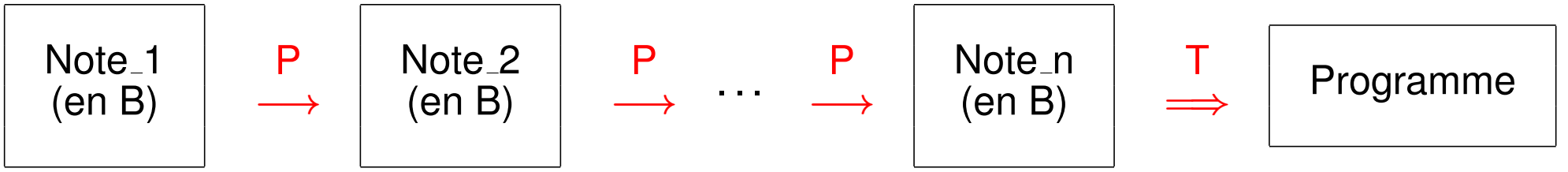
- Entre les notes formelles: raffinements et preuves



- Entre les notes formelles: raffinements et preuves

- Entre Note_n et programme: une TRADUCTION

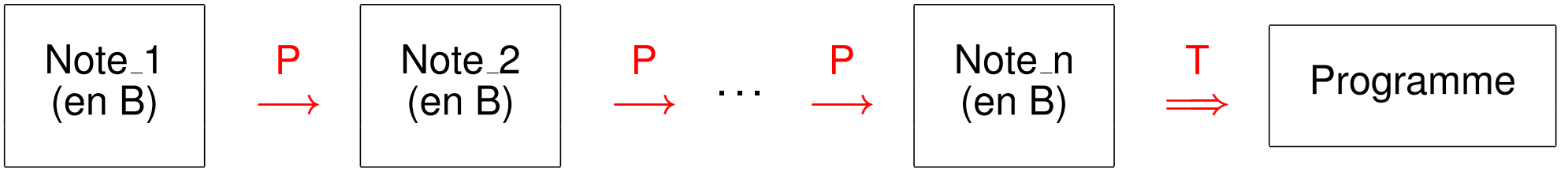
Explications simplifiée de B: Faire des Plans



- Entre les notes formelles: raffinements et preuves

- Entre Note_n et programme: une TRADUCTION

- Les Notes s'appellent maintenant des modèles formels



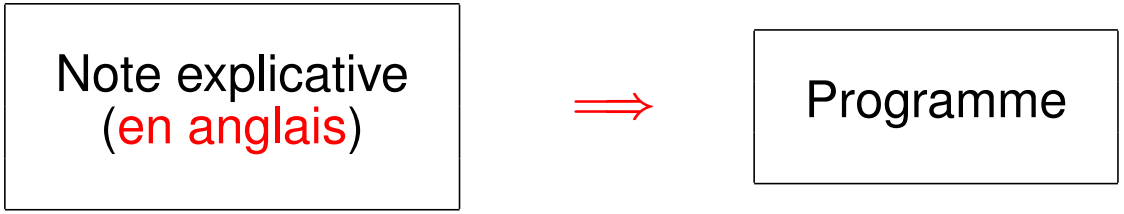
- Entre les notes formelles: raffinements et preuves

- Entre Note_n et programme: une TRADUCTION

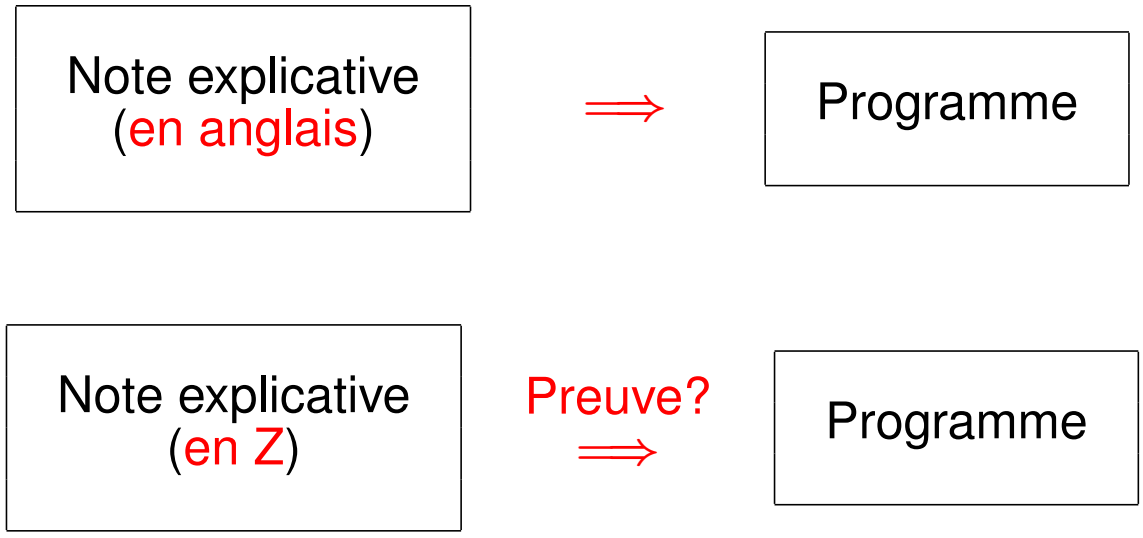
- Les Notes s'appellent maintenant des modèles formels

- Le programmeur devient un modélisateur

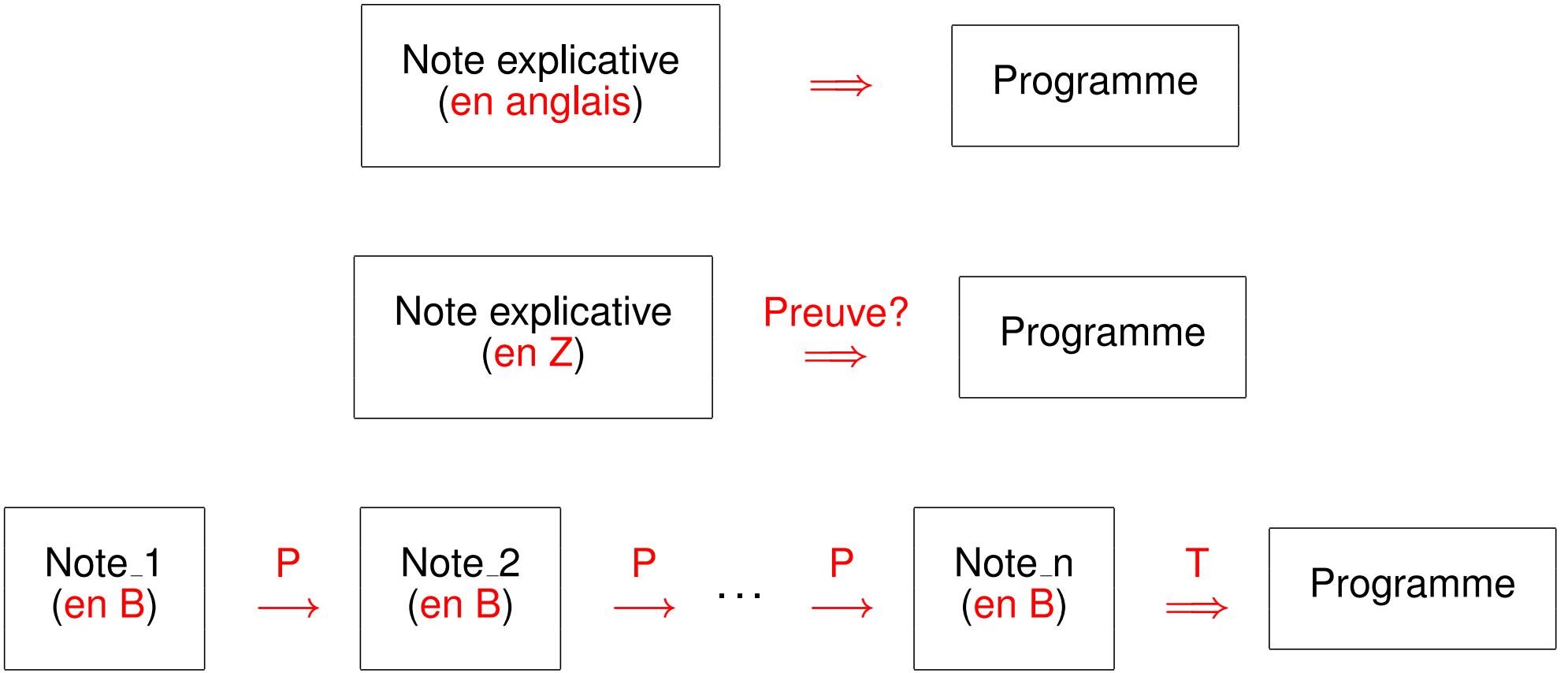
Nouvelle Évolution



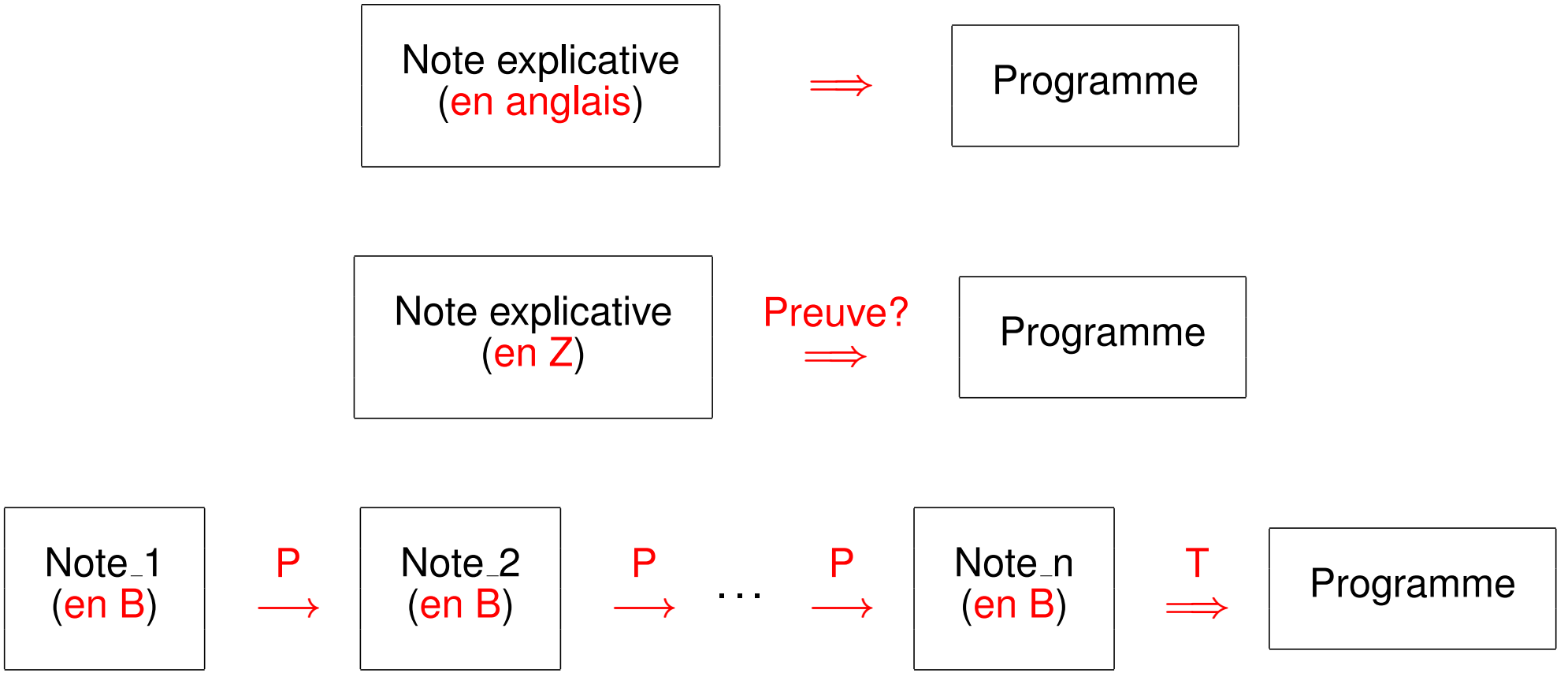
Nouvelle Évolution



Nouvelle Évolution



Nouvelle Évolution



- Mais: Est-ce que ça marche?

Contact Industriel (1)

- Premiers contacts avec la RATP

Contact Industriel (1)

- Premiers contacts avec la RATP

- Au début des années 80, projet d'un métro semi-automatique (RER)

Contact Industriel (1)

- Premiers contacts avec la RATP

- Au début des années 80, projet d'un métro semi-automatique (RER)

- Développement d'un très important système embarqué

Contact Industriel (1)

- Premiers contacts avec la RATP

- Au début des années 80, projet d'un métro semi-automatique (RER)

- Développement d'un très important système embarqué

- Mais les managers ont eu peur de prendre la décision finale

Contact Industriel (1)

- Premiers contacts avec la RATP

- Au début des années 80, projet d'un métro semi-automatique (RER)

- Développement d'un très important système embarqué

- Mais les managers ont eu peur de prendre la décision finale

- Je suis contacté par Claude Hennebert ingénieur de la RATP
  en charge du projet RER

Contact Industriel (2)

- La RATP m’a demandé de faire un audit technique

Contact Industriel (2)

- La RATP m'a demandé de faire un audit technique

- Je devais répondre à la question suivante:
    - Les moyens mis en oeuvre permettent-ils de garantir
      que le produit final correspond bien à sa spécification initiale?

Contact Industriel (2)

- La RATP m'a demandé de faire un audit technique

- Je devais répondre à la question suivante:
    - Les moyens mis en oeuvre permettent-ils de garantir
      que le produit final correspond bien à sa spécification initiale?

- En fait, je n'ai pas pu répondre car je n'ai pas vu de spécifications

Contact Industriel (2)

- La RATP m'a demandé de faire un audit technique

- Je devais répondre à la question suivante:
    - Les moyens mis en oeuvre permettent-ils de garantir
      que le produit final correspond bien à sa spécification initiale?

- En fait, je n'ai pas pu répondre car je n'ai pas vu de spécifications

- Fureur des industriels: mais ils ont bien du s'y résoudre

Contact Industriel (2)

- La RATP m'a demandé de faire un audit technique

- Je devais répondre à la question suivante:
    - Les moyens mis en oeuvre permettent-ils de garantir
      que le produit final correspond bien à sa spécification initiale?

- En fait, je n'ai pas pu répondre car je n'ai pas vu de spécifications

- Fureur des industriels: mais ils ont bien du s'y résoudre

- Finalement le projet a été retardé d'un an

- Après cela, on m’a demandé de faire un cours de spécification.

- Après cela, on m'a demandé de faire un cours de spécification.

- À la mi 80 la RATP se lance dans un métro sans conducteur pour la nouvelle ligne 14

- Après cela, on m'a demandé de faire un cours de spécification.

- À la mi 80 la RATP se lance dans un métro sans conducteur pour la nouvelle ligne 14

- Utilisation de B pour développer les parties critiques du logiciel

- Après cela, on m'a demandé de faire un cours de spécification.

- À la mi 80 la RATP se lance dans un métro sans conducteur pour la nouvelle ligne 14

- Utilisation de B pour développer les parties critiques du logiciel

- Développement de l'outil "Atelier B" entièrement financé par la RATP

- La RATP decide de supprimer les tests unitaires et d’intégration

- La RATP decide de supprimer les tests unitaires et d’intégration

- Octobre 98: lancement de la Ligne 14

- La RATP decide de supprimer les tests unitaires et d'intégration

- Octobre 98: lancement de la Ligne 14

- Depuis lors pas de problèmes avec le logiciel développé avec B

Quelques chiffres concernant le projet Ligne 14

- 86.000 lignes en ADA ont été produites automatiquement

Quelques chiffres concernant le projet Ligne 14

- 86.000 lignes en ADA ont été produites automatiquement

- 27.800 preuves ont été faites

Quelques chiffres concernant le projet Ligne 14

- 86.000 lignes en ADA ont été produites automatiquement

- 27.800 preuves ont été faites

- 92% ont été prouvées automatiquement par l'Atelier B

Quelques chiffres concernant le projet Ligne 14

- 86.000 lignes en ADA ont été produites automatiquement

- 27.800 preuves ont été faites

- 92% ont été prouvées automatiquement par l'Atelier B

- Coût des preuves interactives: 7 homme-mois

Quelques chiffres concernant le projet Ligne 14

- 86.000 lignes en ADA ont été produites automatiquement

- 27.800 preuves ont été faites

- 92% ont été prouvées automatiquement par l'Atelier B

- Coût des preuves interactives: 7 homme-mois

- Les preuves interactives sont moins chères que les tests

- Métros utilisant B pour leurs développements:
    - New York City, Amérique du Sud, Europe, Chine, etc.

Des Hauts et des Bas: les plus (1)

- Métros utilisant B pour leurs développements:
    - New York City, Amérique du Sud, Europe, Chine, etc.

- Projets plus récents en France avec B:
    - Ligne 1 de la RATP à Paris (sans conducteur)

Des Hauts et des Bas: les plus (1)

- Métros utilisant B pour leurs développements:
  - New York City, Amérique du Sud, Europe, Chine, etc.

- Projets plus récents en France avec B:
  - Ligne 1 de la RATP à Paris (sans conducteur)
  - Navette de l'Aéroport Charles de Gaulle (sans conducteur)

    (158.000 lignes en ADA, 43.600 preuves, 96.7% auto)

- L'Atelier B développé par la société Clearsy.

Des Hauts et des Bas: les plus (2)

- L'Atelier B développé par la société Clearsy.

- Un Outil de raffinement developpé par Siemens Transport

Des Hauts et des Bas: les plus (2)

- L'Atelier B développé par la société Clearsy.

- Un Outil de raffinement developpé par Siemens Transport

- Un autre outil de raffinement developpé par Clearsy

Des Hauts et des Bas: les plus (2)

- L'Atelier B développé par la société Clearsy.

- Un Outil de raffinement developpé par Siemens Transport

- Un autre outil de raffinement developpé par Clearsy

- Deux sociétés françaises de logiciel font du B: Clearsy et Systerel

- L'Atelier B développé par la société Clearsy.

- Un Outil de raffinement developpé par Siemens Transport

- Un autre outil de raffinement developpé par Clearsy

- Deux sociétés françaises de logiciel font du B: Clearsy et Systerel

- Elles marchent toutes les deux très bien

- Traduction du B-Book en ... chinois

- B est absent dans: voitures, aviation, espace, nucléaire, etc.

- B est absent dans: voitures, aviation, espace, nucléaire, etc.

- Arguments:

    - Les preuves interactives sont trop difficiles

- B est absent dans: voitures, aviation, espace, nucléaire, etc.

- Arguments:
    - Les preuves interactives sont trop difficiles
    - B est trop loin de la culture de nos ingénieurs

- B est absent dans: voitures, aviation, espace, nucléaire, etc.

- Arguments:
    - Les preuves interactives sont trop difficiles
    - B est trop loin de la culture de nos ingénieurs
    - B est trop cher

- B est absent dans: voitures, aviation, espace, nucléaire, etc.

- Arguments:
    - Les preuves interactives sont trop difficiles
    - B est trop loin de la culture de nos ingénieurs
    - B est trop cher

- Et à la RATP, il y a aussi un important lobby contre B

Modélisation “système”(1)

- Vers les années 2000, après le succès de la ligne 14

Modélisation “système”(1)

- Vers les années 2000, après le succès de la ligne 14

- Je me suis intéressé aux études système

Modélisation “système”(1)

- Vers les années 2000, après le succès de la ligne 14

- Je me suis intéressé aux études système

- Elles sont effectuées par les ingénieurs système

Modélisation “système” (2)

- Déterminer les composants d’un système et leurs relations

Modélisation “système” (2)

- Déterminer les composants d’un système et leurs relations

- Le développement formel avec B commence après ces études

Modélisation “système” (2)

- Déterminer les composants d’un système et leurs relations

- Le développement formel avec B commence après ces études

- Il est effectué sur chaque composant indépendamment des autres

Modélisation “système” (3)

- Que se passe-t-il si des erreurs existent dans les études système?

Modélisation “système” (3)

- Que se passe-t-il si des erreurs existent dans les études système?

- Le développement formel ne les trouve pas en général

Modélisation “système” (3)

- Que se passe-t-il si des erreurs existent dans les études système?

- Le développement formel ne les trouve pas en général

- D’où l’idée de rendre ces études plus formalisées

Modélisation “système” (3)

- Que se passe-t-il si des erreurs existent dans les études système?

- Le développement formel ne les trouve pas en général

- D’où l’idée de rendre ces études plus formalisées

- On voudrait pouvoir effectuer des preuves au cours de ces études

Modélisation “système” (3)

- Que se passe-t-il si des erreurs existent dans les études système?

- Le développement formel ne les trouve pas en général

- D’où l’idée de rendre ces études plus formalisées

- On voudrait pouvoir effectuer des preuves au cours de ces études

- Pour cela le formalisme doit être un peu différent de B

Modélisation “système” (4)

- On doit modéliser un système avec de nombreux composants

Modélisation “système” (4)

- On doit modéliser un système avec de nombreux composants

- Certains d’entre eux deviendront des composants logiciels

Modélisation “système” (4)

- On doit modéliser un système avec de nombreux composants

- Certains d’entre eux deviendront des composants logiciels

- Les autres sont des composants physiques de l’environnement

Modélisation “système” (4)

- On doit modéliser un système avec de nombreux composants

- Certains d’entre eux deviendront des composants logiciels

- Les autres sont des composants physiques de l’environnement

- Une situation où le calcul est essentiellement distribué

Modélisation “système” (5)

- On doit tenir compte des erreurs de certains composants

Modélisation “système” (5)

- On doit tenir compte des erreurs de certains composants

- On doit aussi considérer des contraintes temporelles

Modélisation “système” (5)

- On doit tenir compte des erreurs de certains composants

- On doit aussi considérer des contraintes temporelles

- Tout ceci rend nécéssaire d’étudier un nouveau formalisme

Modélisation “système” (5)

- On doit tenir compte des erreurs de certains composants

- On doit aussi considérer des contraintes temporelles

- Tout ceci rend nécéssaire d’étudier un nouveau formalisme

- Event-B EST NÉ (dans les années 2000-2010)

- Le Professeur Michael Butler m'a parlé de Action System développé en Finlande par Ralph Back and Reino Kurki-Suonio

- Le Professeur Michael Butler m'a parlé de Action System développé en Finlande par Ralph Back and Reino Kurki-Suonio

- De nombreuses idées y ont été incorporées dans Event-B

Un Effort Européen : Event-B et la Plateforme Rodin (1)

- Le Professeur Michael Butler m'a parlé de Action System développé en Finlande par Ralph Back and Reino Kurki-Suonio

- De nombreuses idées y ont été incorporées dans Event-B

- À partir de 2002, il y a eu 4 Projets Européens:
  - Matisse
  - Rodin
  - Deploy
  - Advance

-Plusieurs universités Européennes ont été parties prenantes:

- Southampton et Newcastle en Grande Bretagne,
- Åbo Akademi en Finlande,
- ETH-Zürich en Suisse,
- Düsseldorf en Allemagne.

-Plusieurs universités Européennes ont été parties prenantes:

- Southampton et Newcastle en Grande Bretagne,
- Åbo Akademi en Finlande,
- ETH-Zürich en Suisse,
- Düsseldorf en Allemagne.

- Ainsi que plusieurs sociétés industrielles:

- Siemens, Bosch, SAP, SSF, Alstom, Clearsy et Systerel

-Plusieurs universités Européennes ont été parties prenantes:

- Southampton et Newcastle en Grande Bretagne,
- Åbo Akademi en Finlande,
- ETH-Zürich en Suisse,
- Düsseldorf en Allemagne.

- Ainsi que plusieurs sociétés industrielles:

- Siemens, Bosch, SAP, SSF, Alstom, Clearsy et Systerel

- J'ai aussi reçu une aide considérable de Dominique Cansell

- Le développement de Event-B,

- Le développement de Event-B,

- La construction d'un outil: la Plateforme Rodin,

- Le développement de Event-B,

- La construction d'un outil: la Plateforme Rodin,

- Des études de cas industrielles

- Le leader principal du projet Rodin a été Laurent Voisin avec:
    - Stefan Hallerstede,
    - Thai Son Hoang,
    - Farhad Mehta,
    - FrançoisTerrier

- Le leader principal du projet Rodin a été Laurent Voisin avec:
    - Stefan Hallerstede,
    - Thai Son Hoang,
    - Farhad Mehta,
    - FrançoisTerrier

- Il a ensuite été étendu pendant le projet Deploy chez Systerel

- Le leader principal du projet Rodin a été Laurent Voisin avec:
  - Stefan Hallerstede,
  - Thai Son Hoang,
  - Farhad Mehta,
  - FrançoisTerrier

- Il a ensuite été étendu pendant le projet Deploy chez Systerel

- Avec Laurent Voisin, Nicolas Beauger, Thomas Muller, et Christophe Métayer.

- Beaucoup d'outils annexes (plug-ins) ont été réalisés:
  - Université de Southampton: UML-B, EventB-ADA,Theory,
  - Universié de Düsseldorf: ProB, ProR.

- Beaucoup d'outils annexes (plug-ins) ont été réalisés:
  - Université de Southampton: UML-B, EventB-ADA,Theory,
  - Universié de Düsseldorf: ProB, ProR.

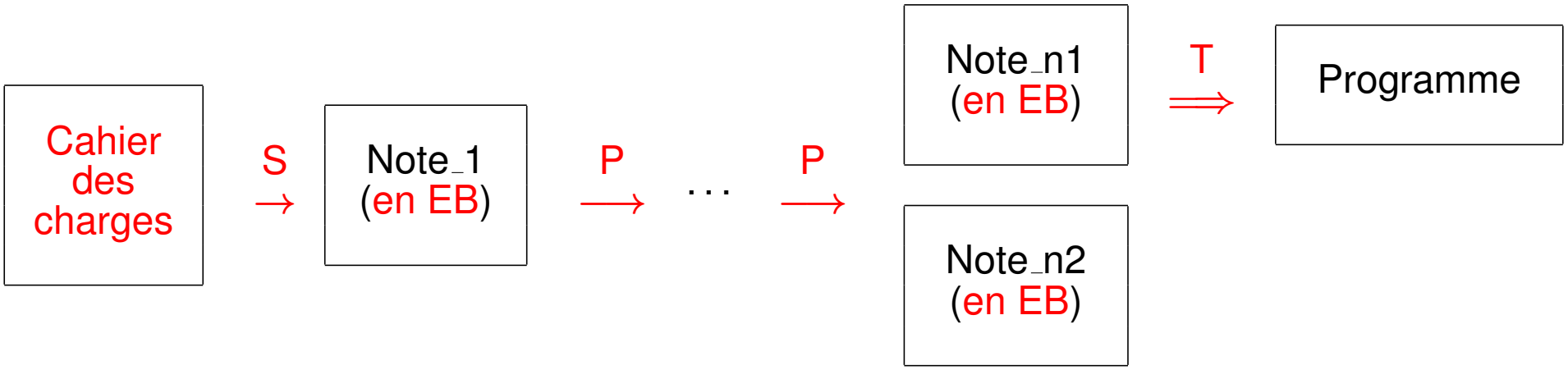
- Cours sur Event-B et la Plateforme Rodin:
  - Australie,
  - Japon, Chine, Malaysie, Inde,
  - Europe,
  - Amériques du Nord et du Sud,
  - Afrique du Nord.

- Introduction explicite du Cahier des Charges

- Introduction explicite du Cahier des Charges
- Introduction de la Stratégie de Raffinement

- Introduction explicite du Cahier des Charges
- Introduction de la Stratégie de Raffinement
- Introduction de l'Environnement dans les modèles

- Introduction explicite du Cahier des Charges
- Introduction de la Stratégie de Raffinement
- Introduction de l'Environnement dans les modèles

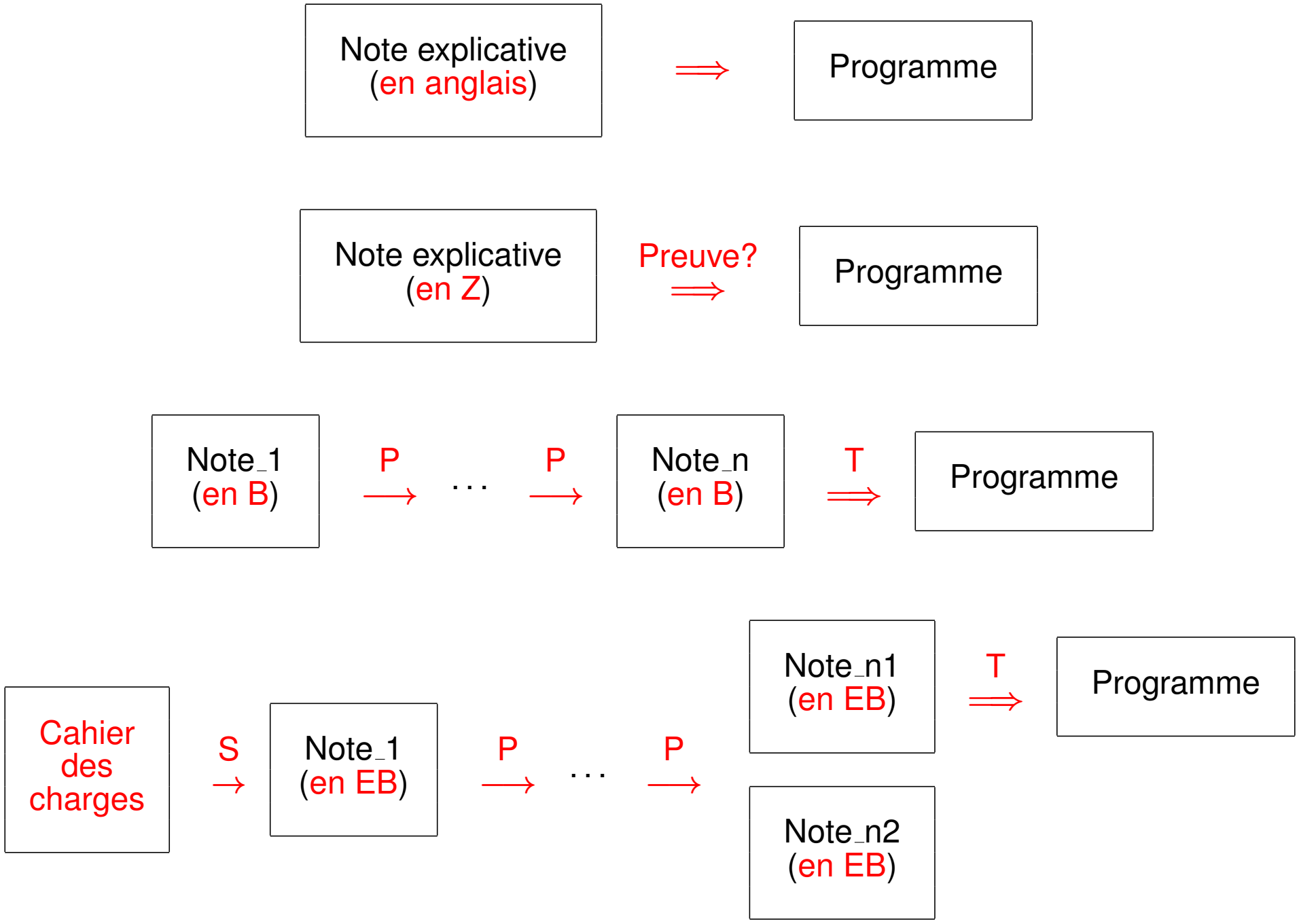


S: Stratégie de raffinement

Note_n1: Modèle final du programme

Note_n2: Modèle final de l'environnement

Evolution Finale (sur 40 ans!!!)



Encouragement du Premier Ministre ... Chinois

Encouragement du Premier Ministre ... Chinois Li Keqiang

搞原始创新，必须更加重视基础研究；推动 IT 业发展的源代码要靠数学

搞原始创新，必须更加重视基础研究；推动 IT 业发展的源代码要靠数学

搞原始创新，必须更加重视基础研究；推动 IT 业发展的源代码要靠数学

Traduction:

En ce qui concerne les innovations originales,

搞原始创新，必须更加重视基础研究；推动 IT 业发展的源代码要靠数学

Traduction:

En ce qui concerne les innovations originales,

accordons davantage d'attention à la recherche fondamentale;

搞原始创新，必须更加重视基础研究；推动 IT 业发展的源代码要靠数学

Traduction:

En ce qui concerne les innovations originales,

accordons davantage d'attention à la recherche fondamentale;

les programmes qui existent dans les applications informatiques

DÉPENDENT DES MATHÉMATIQUES


Event-B
リファインメントモデリングに基づく形式手法

Une autre Évolution: les Systèmes Hybrides (1)

Une autre Évolution: les Systèmes Hybrides (1)

- Plusieurs groupes étudient les possibilités de Event-B:
    - Shanghai University: Wen Su
    - Université de Manchester: Richard Banach

Une autre Évolution: les Systèmes Hybrides (1)

- Plusieurs groupes étudient les possibilités de Event-B:
    - Shanghai University: Wen Su
    - Université de Manchester: Richard Banach
- B and Event-B étaient jusqu'ici utilisés pour modéliser des systèmes discrets

Une autre Évolution: les Systèmes Hybrides (1)

- Plusieurs groupes étudient les possibilités de Event-B:
    - Shanghai University: Wen Su
    - Université de Manchester: Richard Banach

- B and Event-B étaient jusqu'ici utilisés pour modéliser des systèmes discrets

- Mais les systèmes hybrides deviennent de plus en plus importants

Une autre Évolution: les Systèmes Hybrides (2)

- On doit contrôler, au moyen d'interventions discrètes,

  une situation externe en évolution continue.

Une autre Évolution: les Systèmes Hybrides (2)

- On doit contrôler, au moyen d'interventions discrètes,
  une situation externe en évolution continue.

- Les recherches sur Continuous Action System sont très importantes:
  - Ralph Back,
  - Luigia Petre,
  - Ivan Porres

Une autre Évolution: les Systèmes Hybrides (3)

- Les parties continues sont définies à l'aide de functions temporelles

Une autre Évolution: les Systèmes Hybrides (3)

- Les parties continues sont définies à l'aide de functions temporelles

- Ces fonctions sont souvent définies par des équations différentielles

Une autre Évolution: les Systèmes Hybrides (3)

- Les parties continues sont définies à l'aide de functions temporelles

- Ces fonctions sont souvent définies par des équations différentielles

- Et ces équations différentielles sont souvent non résolubles

Une autre Évolution: les Systèmes Hybrides (3)

- Les parties continues sont définies à l'aide de functions temporelles

- Ces fonctions sont souvent définies par des équations différentielles

- Et ces équations différentielles sont souvent non résolubles

- Comment alors prouver certaines propriétés de ces fonctions?

Une autre Évolution: les Systèmes Hybrides (3)

- Les parties continues sont définies à l'aide de functions temporelles

- Ces fonctions sont souvent définies par des équations différentielles

- Et ces équations différentielles sont souvent non résolubles

- Comment alors prouver certaines propriétés de ces fonctions?

- Tout ceci est actuellement du domaine de la recherche.

Exemple: Commande de Trains d'Atterrissage

Schema Simplifié d'un Train d'Atterrissage

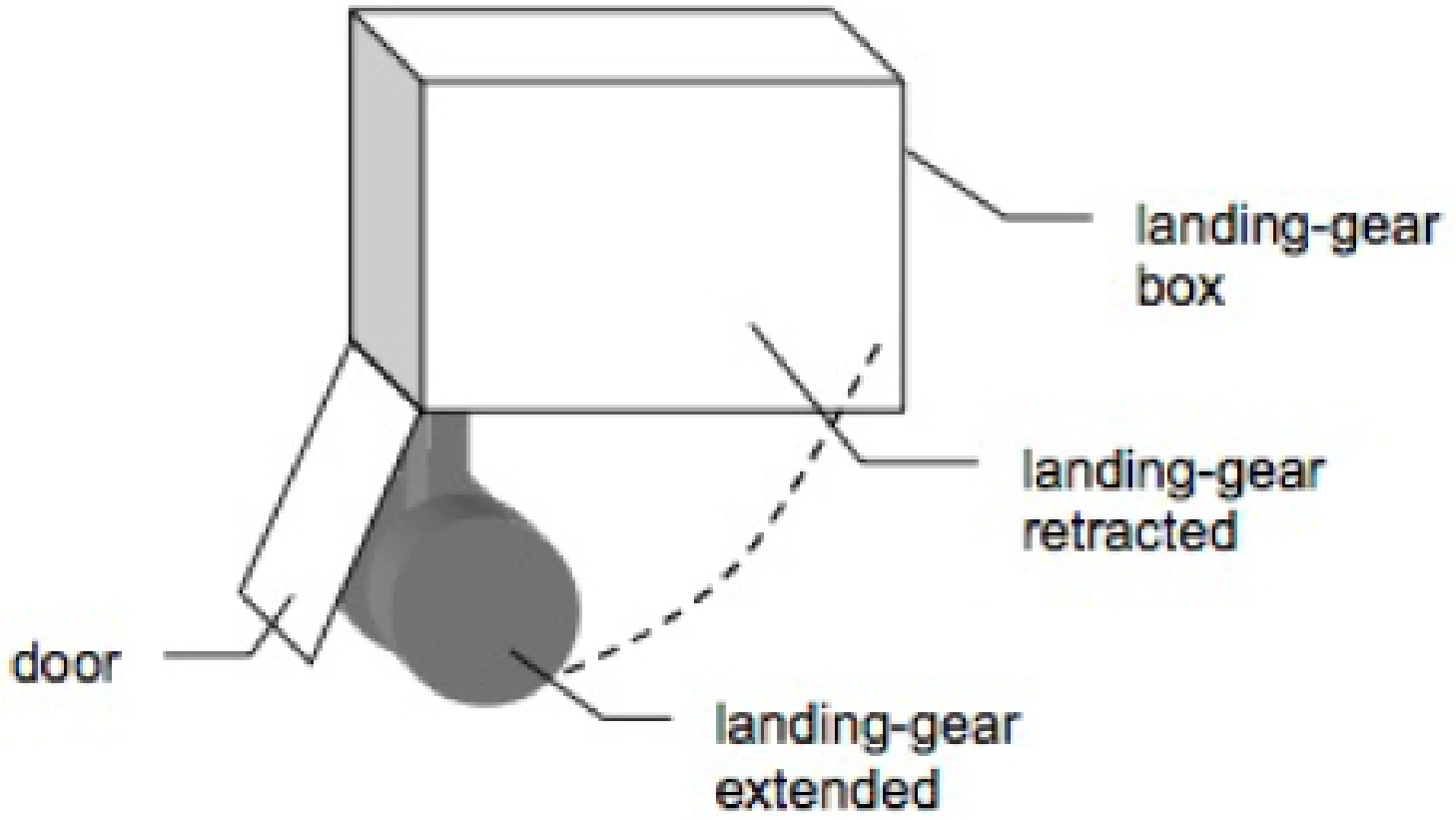
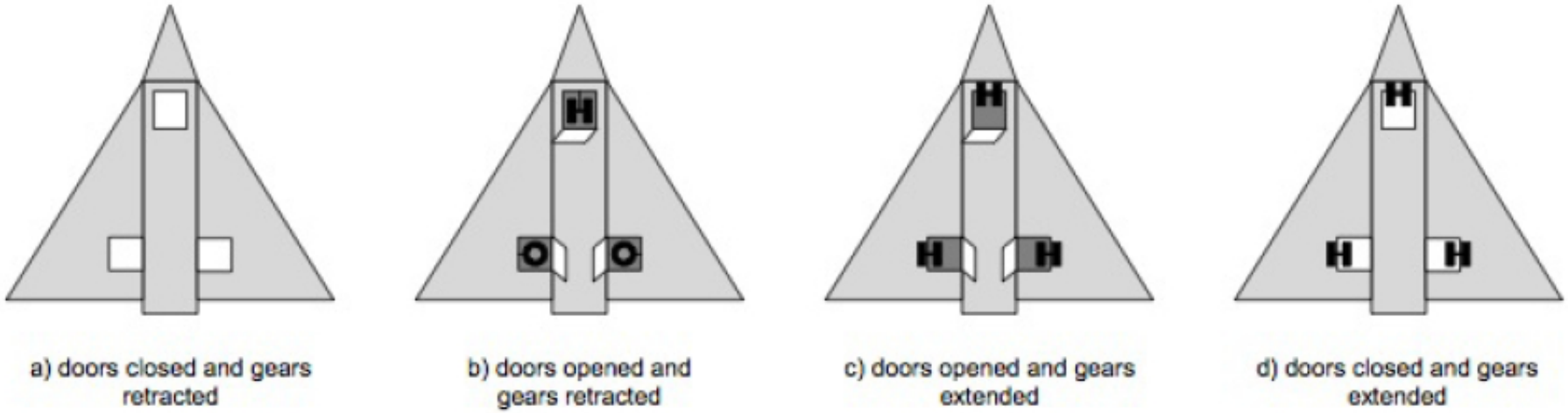


Illustration de la Séquence d'Extension



a) portes fermées et roues rétractées

b) portes ouvertes et roues rétractées

c) portes ouvertes et roues étendues

d) portes fermées et roues étendues

- Le cahier des charges

- La stratégie de raffinement

- Le développement des modèles formels

Quelques éléments du Cahier des Charges (Environnement)

Le système comprend 3 trains (gauche, droite, devant)	ENV-1

Quelques éléments du Cahier des Charges (Environnement)

Le système comprend 3 trains (gauche, droite, devant)	ENV-1

Chaque train comprend des roues qui peuvent être rétractées, étendues ou en mouvement.	ENV-2

Quelques éléments du Cahier des Charges (Environnement)

Le système comprend 3 trains (gauche, droite, devant)	ENV-1

Chaque train comprend des roues qui peuvent être rétractées, étendues ou en mouvement.	ENV-2

Chaque train comprend aussi une porte qui peut être ouverte, fermée ou en mouvement.	ENV-3

Quelques éléments du Cahier des Charges (Environnement)

Le système comprend 3 trains (gauche, droite, devant)	ENV-1
Chaque train comprend des roues qui peuvent être rétractées, étendues ou en mouvement.	ENV-2
Chaque train comprend aussi une porte qui peut être ouverte, fermée ou en mouvement.	ENV-3
Les trains (portes et roues) sont mis en mouvement par l'intermédiaire de pistons hydrauliques.	ENV-4

Quelques éléments du Cahier des Charges (Environnement)

Le système comprend 3 trains (gauche, droite, devant)	ENV-1
Chaque train comprend des roues qui peuvent être rétractées, étendues ou en mouvement.	ENV-2
Chaque train comprend aussi une porte qui peut être ouverte, fermée ou en mouvement.	ENV-3
Les trains (portes et roues) sont mis en mouvement par l'intermédiaire de pistons hydrauliques.	ENV-4
Dans le cockpit, il y a, à la disposition du pilote, une poignée qui peut être en position haute ou basse.	ENV-5

Si les trains sont rétractés et que la poignée va de haut en bas, la séquence d'extension a lieu	FUN-1

Quelques éléments du Cahier des Charges (Fonctionnalités)

Si les trains sont rétractés et que la poignée va de haut en bas, la séquence d'extension a lieu	FUN-1

Séquence d'extension: ouverture des portes, extension des roues, fermeture des portes	FUN-2

Quelques éléments du Cahier des Charges (Fonctionnalités)

Si les trains sont rétractés et que la poignée va de haut en bas, la séquence d'extension a lieu	FUN-1

Séquence d'extension: ouverture des portes, extension des roues, fermeture des portes	FUN-2

- idem dans l'autre sens: rétraction

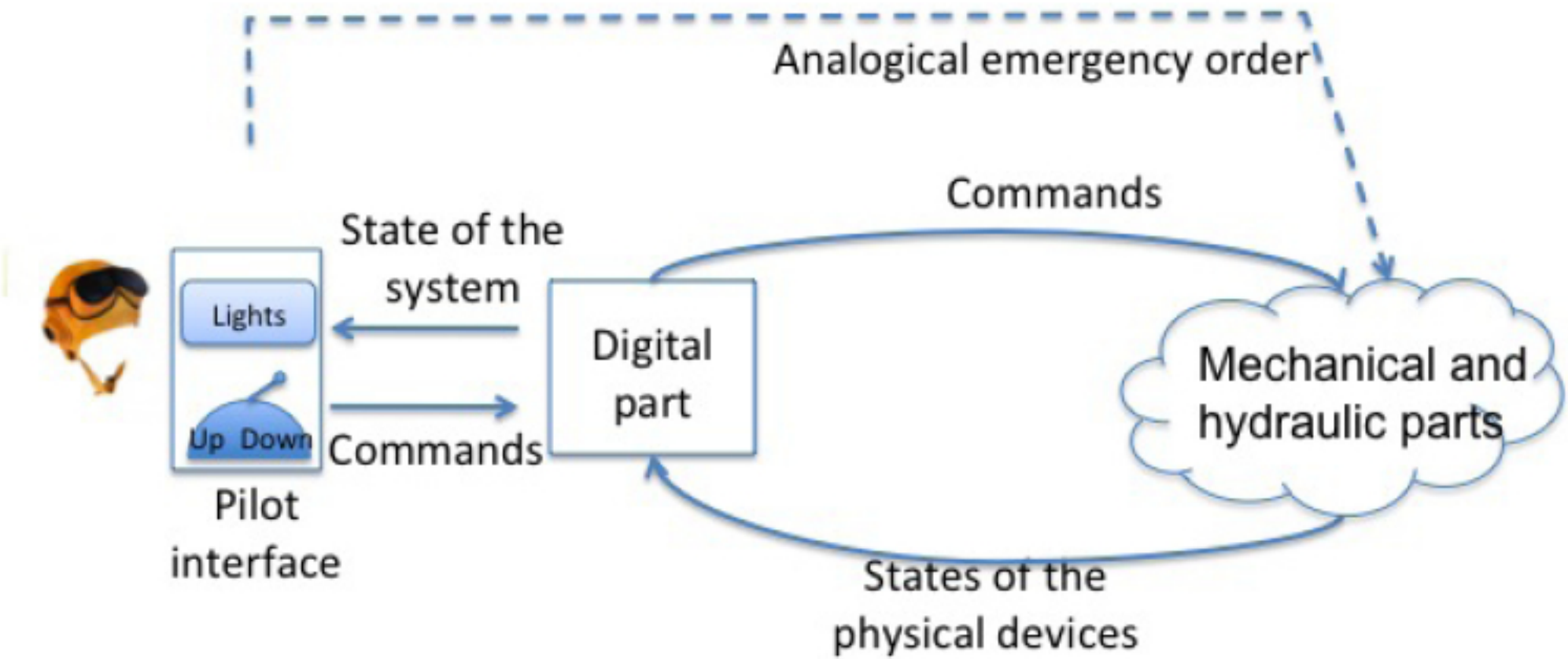
Quelques éléments du Cahier des Charges (Fonctionnalités)

Si les trains sont rétractés et que la poignée va de haut en bas, la séquence d'extension a lieu	FUN-1

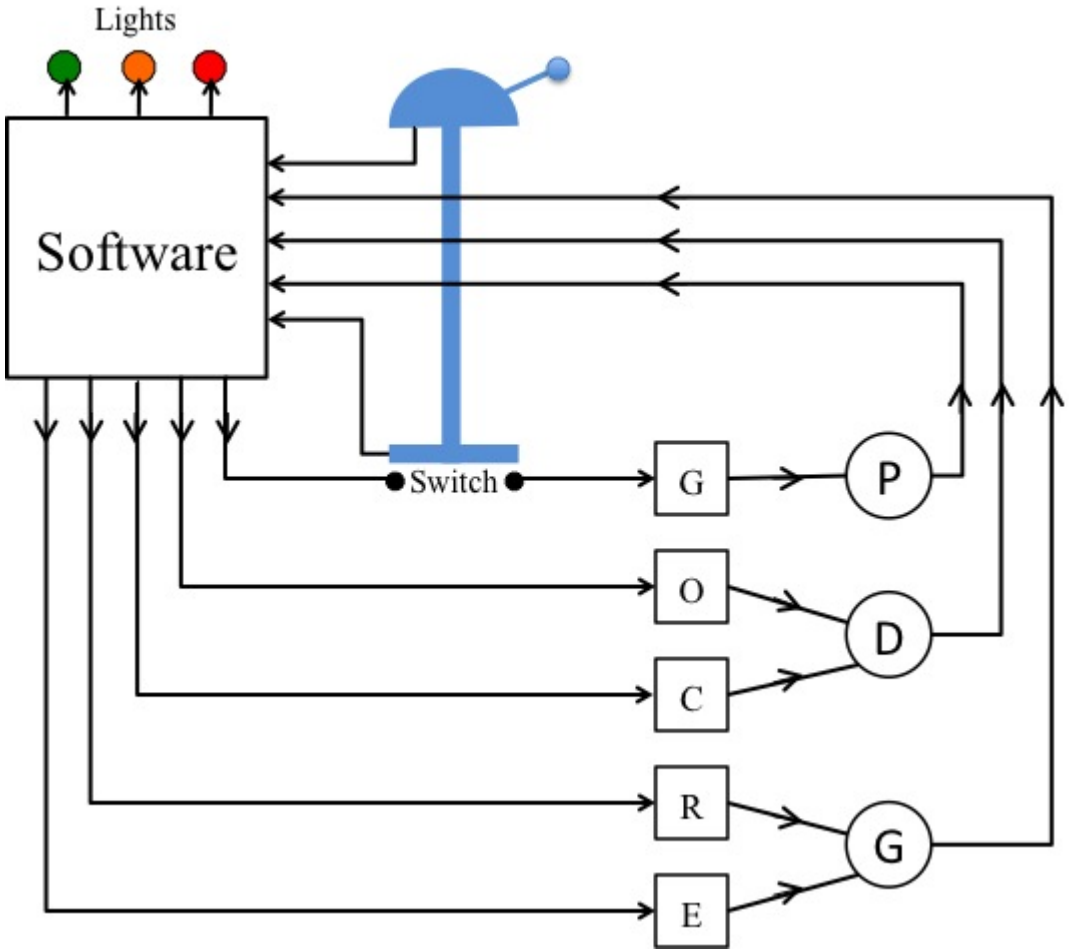
Séquence d'extension: ouverture des portes, extension des roues, fermeture des portes	FUN-2

- idem dans l'autre sens: rétraction

En cours d'extension ou de rétraction, le pilote peut changer la position de la poignée	FUN-3


Analogical emergency order
Commands
State of the system
Lights
Up Down
Commands
Digital part
Mechanical and hydraulic parts
Pilot interface
States of the physical devices

Architecture Détaillée (simplifiée)



G: Electro-valve générale
O: Eectro-valve d'ouverture
C: Electro-valve de fermeture
R: Electro-valve de rétraction
E: Electro-valve d'extension

P: Pression hydraulique
D: Portes
G: Roues

Circuits non pressurisés 2 sec après stimulation	ANM-1

Circuits non pressurisés 2 sec après stimulation	ANM-1

Portes encore fermées 7 sec après stimulation	ANM-2

Circuits non pressurisés 2 sec après stimulation	ANM-1
Portes encore fermées 7 sec après stimulation	ANM-2
Portes encore ouvertes 7 sec après stimulation	ANM-3

Quelques Detection d'Anomalies

Circuits non pressurisés 2 sec après stimulation	ANM-1
Portes encore fermées 7 sec après stimulation	ANM-2
Portes encore ouvertes 7 sec après stimulation	ANM-3
Roues non rétractées 10 sec après stimulation	ANM-4

Quelques Detection d'Anomalies

Circuits non pressurisés 2 sec après stimulation	ANM-1
Portes encore fermées 7 sec après stimulation	ANM-2
Portes encore ouvertes 7 sec après stimulation	ANM-3
Roues non rétractées 10 sec après stimulation	ANM-4
Roues non étendues 10 sec après stimulation	ANM-5

- 21 Environnement (ENV)

- 13 Functionalités (FUN)

- 7 Anomalies (ANM)

- 41 Total

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

1. Synchronisation de la poignée avec le train “unique”

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

1. Synchronisation de la poignée avec le train “unique”

2. Contrôle des portes et des roues par le logiciel

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

1. Synchronisation de la poignée avec le train “unique”

2. Contrôle des portes et des roues par le logiciel

3. Introduction des électro-valves hydrauliques

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

1. Synchronisation de la poignée avec le train “unique”

2. Contrôle des portes et des roues par le logiciel

3. Introduction des électro-valves hydrauliques

4. Introduction des contraintes temporelles

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

1. Synchronisation de la poignée avec le train “unique”

2. Contrôle des portes et des roues par le logiciel

3. Introduction des électro-valves hydrauliques

4. Introduction des contraintes temporelles

...

8. Introduction des 3 trains

Stratégie de Raffinement (simplifiée)

0. Mouvements libres de la poignée, et du train “unique” (abstraction)

1. Synchronisation de la poignée avec le train “unique”

2. Contrôle des portes et des roues par le logiciel

3. Introduction des électro-valves hydrauliques

4. Introduction des contraintes temporelles

...

8. Introduction des 3 trains

- Vérification de la couverture du Cahier des Charges

- Construction progressive des modèles (par raffinements successifs)

- Construction progressive des modèles (par raffinements successifs)

- Preuves systématiques effectuées à chaque étape:
    - conservation d'invariants
    - raffinements corrects
    - absence de bloquage

- Construction progressive des modèles (par raffinements successifs)

- Preuves systématiques effectuées à chaque étape:
    - conservation d'invariants
    - raffinements corrects
    - absence de bloquage

- Confrontation à chaque étape avec d'autres approches:
    - model checking
    - animations

- Construction progressive des modèles (par raffinements successifs)

- Preuves systématiques effectuées à chaque étape:
    - conservation d'invariants
    - raffinements corrects
    - absence de bloquage

- Confrontation à chaque étape avec d'autres approches:
    - model checking
    - animations

- Résultat: plus de 2000 preuves (toutes prouvées automatiquement)

Conclusion

- Z et Event-B essentiellement utilisés dans le milieu universitaire

Conclusion

- Z et Event-B essentiellement utilisés dans le milieu universitaire

- B essentiellement utilisé dans le milieu industriel

- Z et Event-B essentiellement utilisés dans le milieu universitaire

- B essentiellement utilisé dans le milieu industriel

- D'après moi, ceci est du à la méthode de financement:
    - Z initialement développé à Oxford
    - B financé par le projet industriel de la RATP pour la ligne 14
    - Event-B financé par des projets européens

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

- Par un pourcentage systématique d'un grand projet industriel

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

- Par un pourcentage systématique d'un grand projet industriel

- Ça existe pour les oeuvres d'art érigées devant les hôpitaux, etc

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

- Par un pourcentage systématique d'un grand projet industriel

- Ça existe pour les oeuvres d'art érigées devant les hôpitaux, etc

- J'en ai parlé

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

- Par un pourcentage systématique d'un grand projet industriel

- Ça existe pour les oeuvres d'art érigées devant les hôpitaux, etc

- J'en ai parlé ... mais n'ai eu aucun succès

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

- Par un pourcentage systématique d'un grand projet industriel

- Ça existe pour les oeuvres d'art érigées devant les hôpitaux, etc

- J'en ai parlé ... mais n'ai eu aucun succès

- Pourtant ça existe

Une Remarque Finale

- Pourrait-on généraliser la méthode de financement de B?

- Par un pourcentage systématique d'un grand projet industriel

- Ça existe pour les oeuvres d'art érigées devant les hôpitaux, etc

- J'en ai parlé ... mais n'ai eu aucun succès

- Pourtant ça existe ... au Brésil et en Suisse

MERCI BEAUCOUP