Du Cahier des Charges à la Spécification Formelle ?

Jeanine SOUQUIÈRES

Imen SAYAR

DEDALE, LORIA

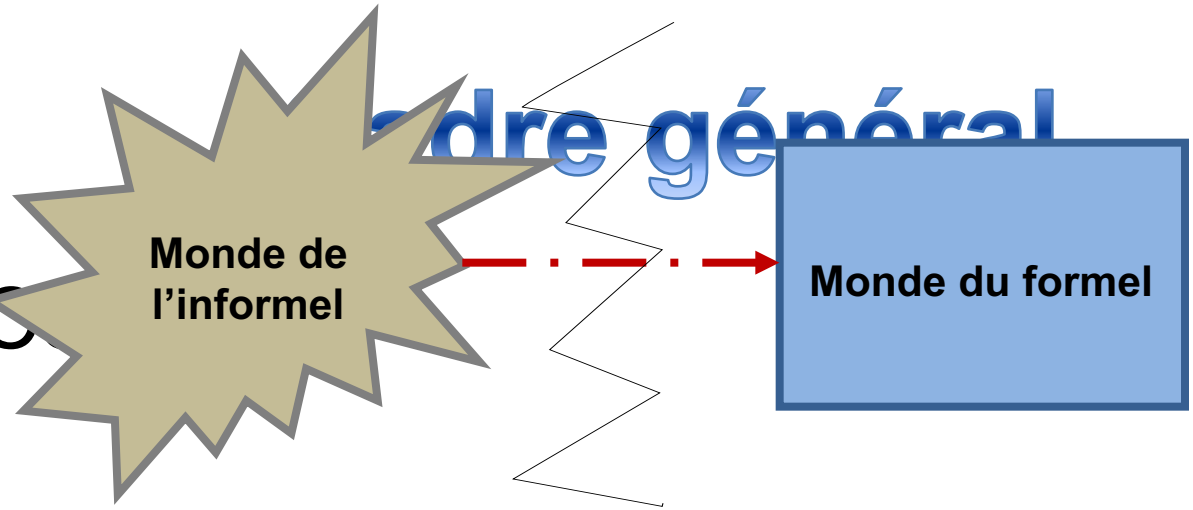
NANCY

Plan

- Cadre général
- Cahier des charges
- Approche adoptée
- Conclusion

Cadre général

Cadre général



- Deux mondes **différents** (informel et formel)
- Des acteurs **différents** (clients, spécifieurs, programmeurs, testeurs, etc.)
- Des langues **différentes**

Client	Spécifieur	Programmeur	Testeur
langue naturelle	langage formel (logique, maths)	langage de programmation (C, Ada, Java,..)	Techniques de test

Cadre général

❑ Contexte

➡ **Interactions entre l'informel et le formel**

- ➢ Systèmes hybrides
- ➢ Vérification et Validation **(V&V)**
- ➢ Traçabilité des exigences dans les modèles formels
- ➢ Intégration de parties formelles dans un processus semi-formel

➡ **Cadre du formel : langage Event-B**

➡ **Cadre de l'informel : Cahier des charges (langue naturelle)**

Cadre général

- Outils

Cadre informel : outil ProR
http://formalmind.com/en/studio
http://www.eclipse.org/rmf/pror/

Cadre formel :

- **Vérification : Plateforme Rodin**
  http://wiki.event-b.org/index.php/Main_Page)
- **Validation**
  - **ProB** (http://stups.hhu.de/ProB/)
  - **JeB** (http://dedale.loria.fr/tiki-index.php?page=Jeb)

Cahier des Charges

Cahier des Charges

- Point de départ du processus de développement de logiciels/systèmes

- CdC
  - **Contrat :** entre différents acteurs (clients, spécifieurs, testeurs, valideurs, etc.)
  - **Référence :** guide contenant tous les détails du futur système

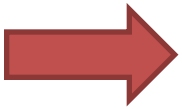
- CdC
  - **Paragraphes**
  - **Figures**
  - **Tableaux**
  - **Parties de programmes**

Mélange de plusieurs concepts

Cahier des Charges

Problèmes liés au CdC

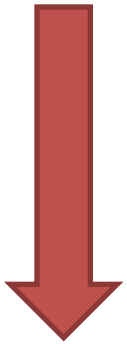
- Ambiguïté => incompréhensible
- Multi-sens : Plusieurs sens pour un même terme/phrase
- Sur-spécification / Absence de détails/ Répétitions
- Absence de trace des exigences dans les modèles développés
- Structure complexe => communication difficile entre acteurs



- Problèmes lors de la **Vérification/Validation**

Cahier des Charges

CdC : **Point de départ** du processus formel



Anomalies (dès le départ)

✖ **Un logiciel/système non forcément valide**

Solution : Prendre soin du Cahier des Charges

Notre approche

Notre approche

Réponses aux questions

➢ Comment préparer le CdC pour être **compréhensible** par tous les **acteurs** dans un processus formel ?

- **Objectif :** faciliter communication des différents acteurs via le CdC

➢ Comment garder une **trace** du **CdC** le long du processus formel de développement de logiciels/systèmes ?

➢ Comment **valider** nos modèles **formels** si on est face à un document **informel** (illisible, ambigu, de grande taille) ?

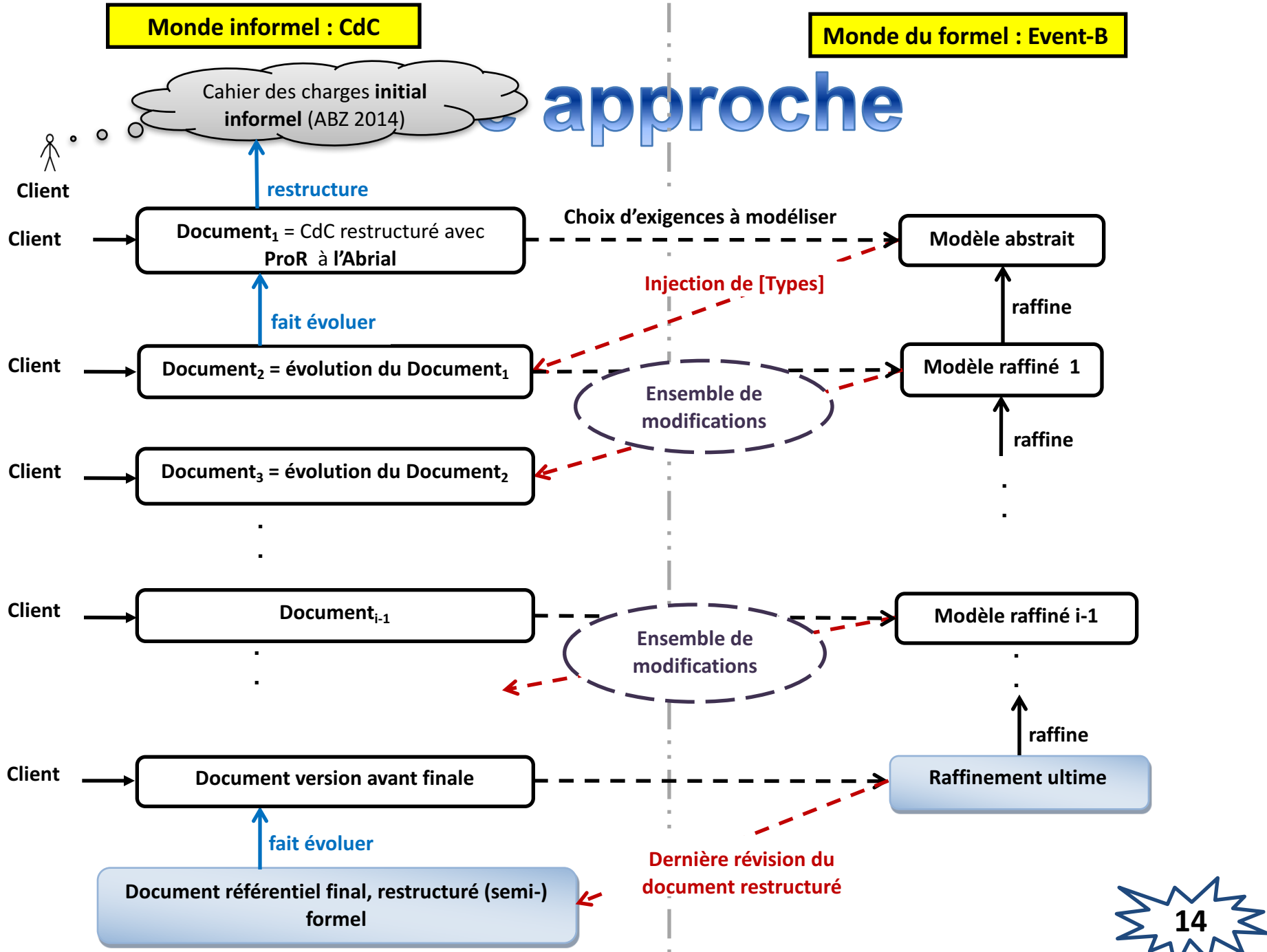
Notre approche

✖ Problème **d'ambiguïté** → ☑ **Restructuration** du CdC [Abrial 2011]
+
Outil **ProR**

✖ **Ecart** entre informel et formel (**incompréhensible**) → ☑ Document restructuré de plus en plus **formel** (mathématique)

✖ **Absence de trace** du CdC → ☑ **Liens** entre exigences-modèles formels
+
Itérations du document restructuré

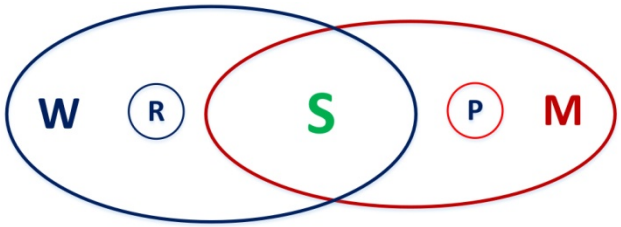
✖ **Vérification** & **Validation** → ☑ **Itérations** du document restructuré
+
Raffinement


Monde informel : CdC
Monde du formel : Event-B
approche
Cahier des charges initial informel (ABZ 2014)
Client
restructure
Client
Document1 = CdC restructuré avec ProR à l'Abrial
Choix d'exigences à modéliser
Modèle abstrait
Injection de [Types]
raffine
fait évoluer
Client
Document2 = évolution du Document1
Ensemble de modifications
Modèle raffiné 1
raffine
Client
Document3 = évolution du Document2
Client
Documenti-1
Ensemble de modifications
Modèle raffiné i-1
raffine
Client
Document version avant finale
Raffinement ultime
fait évoluer
Dernière révision du document restructuré
Document référentiel final, restructuré (semi-) formel

Notre approche

L'outil ProR :

- **Formalmind** (M. Jastram): http://formalmind.com/
- Plugin dans la plateforme Rodin
- Modèle **WRSPM**



- Structure **hiérarchisée** (exigence **Parent** et exigence **Enfant)**
- Introduction de la notion de **lien**
- **Lien** dans ProR
  - Inter-exigences : **Req1|> Req2**
  - Entre exigence et éléments formels : **Req1|> inv x**

Notre approche

Restructuration du CdC : quelques règles [Abrial 2011]

- Texte **explicatif** (le comment ?)
- Texte **référentiel** (le quoi ?)

Règle 1 : phrases courtes, lisibles et non ambiguës avec *un seul objet*

« *Maneuvring* ***doors*** *consists on opening or closing them* »
=> **objet** : doors

Règle 2 : un seul objectif par phrase

« ***Maneuvring*** *doors consists on opening or closing them* »
=>**objectif** : maneuvring doors

Notre approche

Règle 3 : exigences **classifiées** selon leur centre d'intérêt : **FUN**, **EQU, DEL, FAIL**,…

« **EQU-2-1 (Pilot Interface) :** Pilot interface contains green, orange and red lights and an Up/Down handle

=> équipements liés à l'interface pilote

Règle 4 : exigences **hiérarchisées** selon niveau de description

FUN-Light :	Lights indicate doors and gears positions	**Exigence parent**
FUN-Light3:	When gears are locked down, the green light is on	**Exigence enfant**

Notre approche

Modification du document restructuré

- Modification document restructuré

➢ **formel :** des modèles formels Event-B

- Injection des **[Types]**
- Ajout de liens exigences-éléments formels

« *Maneuvring [Doors] consists on [open_doors] or [close_doors]* »

Sets (au sens Event-B)

Event (au sens Event-B)

➢ **informel :** document lui-même

- Ajout de liens inter-exigences
- Suppression d'exigences (contradictions,..)
- Ajout de contraintes implicites

Evolution du document restructuré dans le processus formel

CdC init : ABZ 2014

Landing gear system

Frédéric Boniol and Virginie Wiels

ONERA-Toulouse, 2 av. E. Belin, BP 4025, 31055 Toulouse France
{firstname.name}@onera.fr

Abstract. This document presents the landing system of an aircraft. It describes the system and provides some of its requirements. We propose this case study as a benchmark for techniques and tools dedicated to the verification of behavioral properties of systems.

1 Introduction

This document presents a landing system. It describes the system and provides some of its requirements. We propose this case study as a benchmark for techniques and tools dedicated to the verification of behavioral properties of systems.

The landing system is in charge of maneuvering landing gears and associated doors. The landing system is composed of 3 landing sets: front, left and right. Each landing set contains a door, a landing-gear and associated hydraulic cylinders. A simplified schema of a landing set is presented in Figure 1.

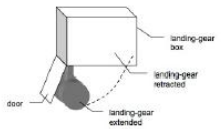


Fig. 1. Landing set

The system is controlled digitally in nominal mode and analogically in emergency mode. In this case study, we do not consider the emergency mode. However, in order to allow the pilot to activate the emergency command, the system has to elaborate health parameters for all the equipments involved in the landing gear function. This health monitoring part is in the scope of the case study.

In nominal mode, the landing sequence is: open the doors of the landing gear boxes, extend the landing gears and close the doors. This sequence is illustrated

Doc1 = CdC init restructuré (Abrial)

Requirements Document

ID	Description
	/* This requirements document results from restructuration of paper "Landing gear System" (Frederic Boniol and Virginie Wiels) appeared in ABZ 2014, it consists on reorganizing it into : (1) Functional constraints (preceeded by label "FUN") , (2) Constraints related to the system equipements (preceeded by label "EQU"), (3) Delays constraints related to the Time concept (preceeded by label "D
	/* The objective of this requirements docum forgetting requirements when developing fo traceability between the requirements and t between requirements is important to garan
FUN-G	The landing system is in charge of maneuvri associated doors
FUN-G-1	Maneuvring landing gears consists on exter reversing their mouvement
FUN-G-2	Maneuvring doors consists on opening or cl
EQU-1	Landing system is composed of 3 sets: fron
EQU-1-1	Each landing set contains : a door, a landing hydraulic cylinders
FUN-1	There are 2 controlling ways of the landing g analogically
FUN-2	Landing gears system state can be either in emergency mode
FUN-3	When the system is in nominal mode, it is co
FUN-4	When the system is in emergency mode it is
FUN-5	The system must elaborate health paramete involved in the LG function according to ther emergency command
FUN-6	In nominal mode, landing sequence consist gears and closing doors
FUN-7	In nominal mode, the retracting sequence co retracting landing gears and then closing do
EQU-2 (System Architecture)	The system is composed of 3 parts : pilot in mechanical part
EQU-2-1 (Pilot Interface)	Pilot interface contains green, orange and r handle
FUN-Light	Lights indicate doors and gears positions
FUN-Light1	Every light can be "on" or "off"
FUN-Light2	All lights are "off" when gears are locked up
FUN-Light3	When gears are locked down, the green ligh
FUN-Light4	When gears are maneuvring, the orange ligh
FUN-Light5	When the landing gears system is failed, the

Requirements Document

ID	Description	Comments	Previous_ID	Type Source Target
DATE	Thursday, November 27, 2014 : Modification of the old restructerd document (july 01, 2014)			
GENERAL DATA	/* This requirements document results from restructuration of paper "Landing gear System" (Frederic Boniol and Virginie Wiels) published in ABZ 2014, it consists on reorganizing it into : (1) Functional constraints (preceeded by label "FUN") , (2) Constraints related to the system equipements (preceeded by label "EQU"), (3) Delays constraints related to the Time concept (preceeded by label "DEL"), (4) Failure constraints describing possible failures of the system equipements, (preceeded by label "FAILURE") */ (date: 01/07/2014)			
OBJECTIVE	/* The objective of this requirements document is to avoid risks of forgetting requirements when developing formal models, to ensure traceability between the requirements and their formalisation. Links between requirements is important to garantee coherence of models */			
FUN-G	The landing system is in charge of maneuvring [Gears] and their associated [Doors]			
FUN-G-1	Maneuvring [Gears] consists on [extend_gears], [retract_gears] or [reverse] their mouvement			
FUN-G-2	Maneuvring [Doors] consists on [open_doors] or [close_doors]			
Gears_Pos	[gears_pos] can be either in [g_retracted] or in [g_extended] [Positions]	Added for explanation (extracted constraint from implicit descriptions)		
Doors_pos	[doors_pos] can be [open] or [closed]	Added for explanation (extracted constraint from implicit descriptions)		
FUN-init-pos	Initially, gears are [g_extended] and system is in [nominal] [Mode]	Added for initialisation (decision taken by the developer)		
LS-EQU-1	Landing system is composed of 3 sets: [front], [left] and [right]	LS = Landing Set	EQU-1	
LS-EQU-1-1	Each [Landing_set] contains : a [door], a [landing_gear] and associated hydraulic [CYLINDER]s		EQU-1-1	
FUN-1	There are 2 [Controlling_Way]s of the landing			

Doc2 = Doc 1 + [Types] + quelques modifications

Conclusion

Conclusion

Point de départ (document restructuré) **facile à comprendre** : forme mathématique simplifiée

Document restructuré **accessible** par **tous les acteurs**

Trace des exigences dans les **modèles formels** (liens exigences-éléments formels fournis par **ProR**)

Validation **simplifiée** (exigences décrivant des scénarios de validation)

L'existence des outils (ProR plugin de Rodin) facilite la **restructuration** et la **traçabilité**

Conclusion

- Interactions entre informel et formel
- Traçabilité des exigences
- Alternance entre le document informel et modèles formels Event-B
- Document informel se rapproche pas-à-pas du formel

Travaux en cours

- Validation des modèles formels en cours de développement
  - Document référentiel restructuré
  - Classification des exigences
    - **- Hypothèses**
    - **- Obligations**
    - **- Données**
    - **- Comportements**
    - **- Fonctionnalités**
  - Validation décomposée → catégorie exigence concernée

Obligation => **invariants** et **axioms**

Fonctionnalités => **events**

…

Données => **Constants, Sets, Variables**

MERCI