Reverse-Engineering Autopilot Behavior on the A340-200/300. The Anatomy of a Modern Autopilot

Denis Javaux

Work Psychology Department
University of Liège
4000 Sart-Tilman, Belgium
d.javaux@ilg.ac.be

Abstract

A rigorous and accurate method for reverse-engineering autopilot behavior from its description in the aircraft operational manual (FCOM) has been developed. The method has been applied to the A340-200/300 in the framework of a contract with Airbus Industrie whose goal was to study pilots' knowledge of autopilot behavior.

Introduction

There has been a growing need in the HF automation community to gain access to high-level descriptions of automation behavior. These descriptions are required for various purposes such as studying pilots knowledge of automation (Javaux and Olivier 2000), comparing autopilot specifications against plausible mental models (Rushby 2002), validating minimal safe mental models of autopilot behavior (Crow, Javaux and Rushby 2000), examining autopilots for consistent behavior (Degani 1996), looking for error-prone designs (Degani 1996, Leveson and Palmer 1997) and predicting automation surprises (Crow, Javaux and Rushby 2000, Javaux 2002, Rushby 2002) or reducing automation complexity (Vakil and Hansman 2002).

Method

The reverse-engineering method presented here is general and can be applied to any past or present autopilot, provided an operational manual is available. It draws on ideas first introduced by (Sherry et al 1997). It consists of eight steps that must be performed sequentially (fig. 1). Each step outputs information that is used by the next ones. Guidelines have been defined for each step.

Figure 2 below shows an example of output from step 2, where a small paragraph of the A340-200/300 FCOM (autoflight chapter) has been segmented into 3 informational zones that contain information relevant to autopilot behavior (203 such paragraphs were found in the 156 pages of the A340-200/300 autoflight chapter and segmented into 555 informational zones).

Reverse-Engineering Method

1. extraction of paragraphs
2. segmentation of paragraphs into informational zones
3. translation into logical expressions
4. identification of conditions
5. semantic checking and normalization
6. integration of logical expressions
7. validation of scenarios
8. representation of scenarios

Figure 1. The 8 steps of the reverse-engineering method

DISENGAGEMENT CONDITIONS

The CLB mode disengages if one of the following occurs:
① NAV mode is lost or disengaged (OP CLB engages)
② Another vertical mode engages.
③ The pilot selects an altitude on the FCU that is lower than the aircraft present altitude. V/S (FPA) engages on current V/S (or FPA).

Figure 2. Segmentation into informational zones

The information found in the informational zones is then translated into accurate logical expressions. The expressions for the informational zones of fig. 2 are shown in table 1. 736 such elementary logical expressions were found in the A340-200/300 FCOM autoflight chapter.

SRC	Transition	Logical expression
S70,1	CLB disengagement	(NAV disengagement)
S70,1	OPEN CLB engagement	(CLB engaged) and (NAV disengagement)
S70,2	CLB disengagement	(other vertical mode engagement)
S70,3	CLB disengagement	(FCU selected altitude below A/C altitude)
S70,3	V/S-FPA engagement	(CLB engaged) and (FCU selected altitude below A/C altitude)

Table 1. Logical expressions for the information found in figure 2.

The reverse-engineering process then continues by normalizing the logical expressions (i.e., ensuring they all rely on the same basic set of predicates and arguments) and integrating them into independent mode or autopilot state transition scenarios. Transition scenarios correspond to single, independent and operationally meaningful autopilot behaviors such as 'ALT engagement when reaching the target altitude' or 'OP CLB engagement with the ALT selector knob'. 302 such independent transition scenarios (or autopilot behaviors) were found on the A340-200/300.

Results

The table below shows how the 302 transition scenarios are distributed within the different families of mode and autopilot behaviors on the A340-200/300. There are for example 13 independent scenarios for engaging the V/S FPA mode.

VERTICAL	arm	disarm	eng	diseng
SRS			2	3
OP CLB			4	4
OP DES			1	4
CLB	4	7	3	6
DES	3	6	2	6
V/S FPA			13	5
ALT*			1	3
ALT CSTR*			1	4
ALT CRZ*			1	4
ALT	1	2	2	1
ALT CSTR			1	3
ALT CRZ			1	3
G/S*			1	4
G/S	1	4	1	5
FINAL	1	6	1	7

SYSTEMS	arm	disarm	eng	diseng
AP			3	11
FD			3	4
A/THR	5	6	4	6

LATERAL	arm	disarm	eng	diseng
HDG TRK			7	1
NAV	3	6	4	3
LOC*			1	4
LOC	2	4	1	5
APP NAV	1	5	2	7
GA TRK			1	1
RWY			1	1
RWY TRK			1	1

COMMON	arm	disarm	eng	diseng
TAKE OFF			1	5
GO AROUND			1	4
LAND			1	2
FLARE			1	1
ROLL OUT			1	
FINAL APP	1	6	1	8

APPROACH	arm	disarm	eng	diseng
PREC. APP	1	4	1	5
N.PREC.APP	1	6	1	8

Table 2. Distribution of the 302 transition scenarios

The figures below depict the results obtained after a more detailed analysis of the data contained in table 2.

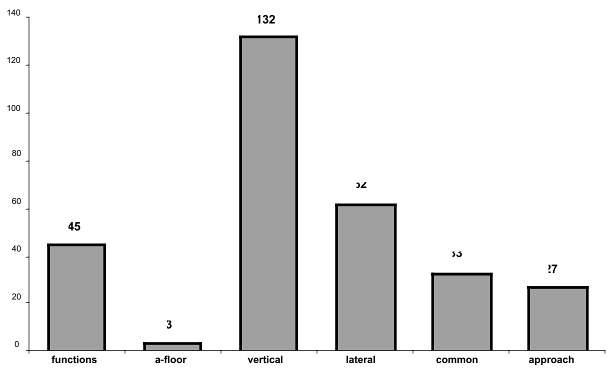

Figure 3. Number of scenarios per family of modes

Figure 3 shows that vertical modes display the most transition scenarios. This correlates well with the general opinion that autopilot behavior is more difficult to understand and master in the vertical channel.

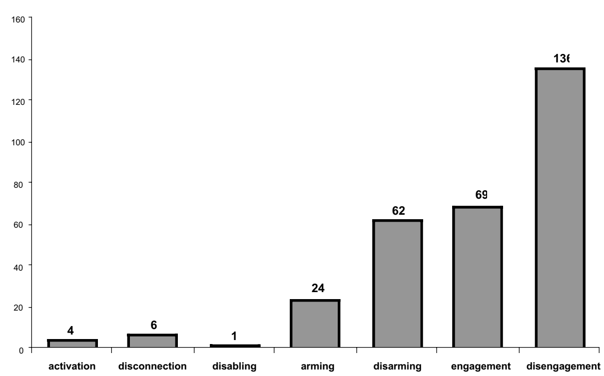

Figure 4. Number of scenarios per type of transitions

Figure 4 indicates that there are more ways of disarming or disengaging a mode or function than there are ways of arming or engaging them.

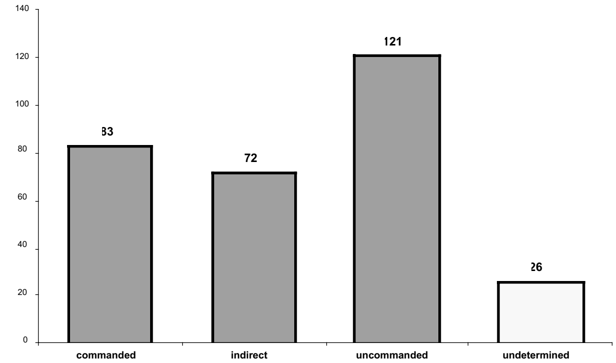

Figure 5. Number of scenarios per category of transitions

Figure 5 finally shows that nearly 70% of the transition scenarios correspond to an indirect or uncommanded transition. They occur without any direct pilot intervention.

References

Crow, J., Javaux, D., and Rushby, J. (2000). Models and Mechanized Methods that Integrate Human Factors into Automation Design. In K. Abbott, J.J. Speyer, and G. Boy (eds), Proceedings of HCI-AERO'2000, September 27-29, Toulouse, France: Cepadues Editions.

Degani, A. (1996). Modeling Human-Machine Systems: On Modes, Error, and Patterns of Interaction. Ph. D. thesis, Georgia Institute of Technology.

Javaux, D. & Olivier, E. (2000). Assessing and Understanding Pilots’ Knowledge of Mode Transitions on the A340-200/300. In K. Abbott, J.J. Speyer, and G. Boy (eds), Proceedings of HCI-AERO'2000, September 27-29, Toulouse, France: Cepadues Editions.

Javaux, D. (2002) A Method for Predicting Errors when Interacting with Finite State Machines. In D. Javaux (ed.). Human Error, Safety, and Systems Development in Aviation. Special issue of Reliability Engineering and System Safety, Elsevier.

Leveson, N.G. & Palmer, E.A. (1997). Designing Automation to Reduce Operator Errors. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Orlando, FL.

Rushby, J. (2002). Using model checking to help discover mode confusions and other automation surprises. In D. Javaux (ed.). Human Error, Safety, and Systems Development in Aviation. Special issue of Reliability Engineering and System Safety, Elsevier.

Sherry, L., Feary, M., Polson, P.G., & Palmer, E. (1997). Analysis of the Behavior of a Modern Autopilot. Prepared for NASA under contract NAS1-20219. Honeywell Publication No. C69-5370-009.

Vakil, S., & Hansman, R.J. (2002). Approaches to Mitigating Complexity-Driven Issues in Commercial Autoflight Systems. In D. Javaux (ed.). Human Error, Safety, and Systems Development in Aviation. Special issue of Reliability Engineering and System Safety, Elsevier.