ETH+ Workshop 7-8 septembre 2020

« Faut-il supprimer l'erreur ? »

La valeur des erreurs à l'heure de la robotique et de l'IA

Valeur des erreurs en ingénierie spatiale : exemple des lanceurs spatiaux

Patrick FARFAL

PatSys[1], conseil et formation en systèmes

Dans l'industrie des lanceurs spatiaux, les erreurs sont à la fois fréquentes et peu nombreuses ; encore faut-il savoir de quoi l'on parle : les erreurs sont fréquentes, parce qu'inévitables et liées à l'activité humaine en ingénierie système, c'est-à-dire au cours du processus de conception – développement – réalisation – validation des lanceurs, et sont en général corrigées ; elles sont rares dans la phase opérationnelle d'utilisation commerciale, pourtant elles existent et alors leur coût est très élevé.

La valeur des erreurs sera abordée en distinguant les « objets » et le « projet », autrement dit les lanceurs eux-mêmes et l'ingénierie système associée. Nous nous limitons aux équipements embarqués, électriques, électroniques, hydrauliques…

Un lanceur n'est au fond qu'un énorme accélérateur de charge utile (satellite, sonde, capsule habitée) mais autonome, donc bourré d'électronique, de logiciels, et d'algorithmes d'un niveau mathématique élevé (ce n'est pas encore de l'IA, qui, selon l'un de ses créateurs, est définie comme capable de « tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains car elles demandent des processus mentaux de haut niveau ») ; ces algorithmes de conduite du vol sont complexes et nécessitent une validation poussée, parce qu'ils sont sujets à des erreurs, principalement de conception. Les autres spécificités d'un lanceur sont le coût, l'obligation d'explorer tout le domaine de vol dès le premier essai, et la sanction, qui est binaire : « sanction binaire » (*success or fail*) sous-entend intrinsèquement que le lanceur peut rencontrer un échec, ce qui milite encore, ainsi que le coût de l'échec éventuel, en faveur d'une validation poussée.

Les erreurs, et pas seulement les erreurs logicielles, les défauts de conception de circuits, les défaillances des techniques d'assemblage de composants…, sont inévitables au long du processus d'étude, de développement, de réalisation, de validation ; on y remédie en mettant en œuvre les principes de l'ingénierie système, laquelle est à la fois approche interdisciplinaire et ensemble de moyens rendant possible la réalisation de systèmes satisfaisant leurs spécifications (donc les besoins du Client) : le déroulement sans faille des différentes phases du processus, associé aux revues de projet, en est la condition.

Néanmoins, le processus peut laisser échapper des insuffisances (identifiées mais « impassées » : Challenger), parfois découvertes tardivement, voire trop tard, à savoir les interactions ou couplages cachés (premier tir d'Ariane 5) ; cela ruine le rêve démesuré de ceux qui pensent réduire le processus d'ingénierie système à un ensemble de logiciels qu'il suffirait d'activer en appuyant sur des boutons les uns après les autres pour que tout se déroule comme prévu : une logique implacable (« mathématique ») ne suffit pas, la capacité de synthèse des équipes reste indispensable.

La valeur d'une erreur, au sens d'utilité, est évidente en développement (elle sécurise les processus), salutaire (hormis les accidents humains) si elle est découverte très tardivement (le premier échec d'Ariane 5 a été suivi d'une revue de projet poussée à l'extrême pendant 5 trimestres). Dans certains cas, d'ailleurs, ce que l'on appelle à tort l'erreur (y compris en anglais), et qui est en réalité un écart, est la base même du fonctionnement de certains systèmes : c'est le cas des automatismes embarqués (de guidage, de pilotage…) dont les lanceurs sont truffés.

L'ingénierie système s'enrichit de ses erreurs : l'illustration en est la roue de William E. Deming, le PDCA : Plan-Do-Check-Act (ou Adjust) - (Planifier-Réaliser/Effectuer-Vérifier-(Ré)Agir/Corriger), des années 50.

[1] 25 rue Jean Leclaire, 75017 Paris, pfarfal.patsys@sfr.fr

ETH+ Workshop, September 7-8, 2020

"Should we delete the Error?"

The value of Errors at the age of Robotics and AI

Value of errors in space engineering: example of space launch vehicles

Patrick FARFAL

PatSys[2], consulting and systems training

In the space launcher industry, errors are both frequent and few in number; but one must also know what we are talking about: errors are frequent, because they are inevitable and linked to human activity, in systems engineering, i.e. during the process of design - development - realization - validation of launch vehicles, and are generally corrected; they are rare in the operational phase of commercial use, yet they do exist, so their cost is very high.

The value of errors will be addressed by distinguishing between the "objects" and the "project", in other words the launch vehicles themselves and the associated system engineering. We will only deal with on-board systems, electrical, electronic, hydraulic, … equipment.

A launch vehicle is basically just a huge accelerator of payload (satellite, probe, manned capsule) but autonomous, therefore full of electronics, software, algorithms, of a high mathematical level (it is not yet AI, which according to one of its creators defines it as capable of "tasks that are, for the moment, performed more satisfactorily by human beings because they require high level mental processes"); these flight control algorithms are complex and require extensive validation, because they are subject to errors, mainly design errors. The other specificities of a launch vehicle are cost, the need to explore the entire flight domain at the very first flight, and the sanction, which is binary: "binary sanction" (success or failure) intrinsically implies that the launch vehicle may fail, which again militates, as does the cost of the possible failure, in favor of in-depth validation.

Errors, and not only software errors, circuit design flaws, component assembly technique failures..., are inevitable throughout the study, development, production and validation process; they are remedied by implementing the principles of systems engineering, which is both an interdisciplinary approach and a set of means making it possible to produce systems that meet their specifications (and therefore the Customer's needs): the smooth running of the various phases of the process, associated with project reviews, is the condition for this.

Nevertheless, the process can let inadequacies (identified but "skipped": e.g. Challenger), sometimes discovered late, or even too late, such as hidden interactions or couplings (e.g. first Ariane 5 launch); this spoils the unbounded dream of those who think they can reduce the systems engineering process to a set of software programs that just need to be activated by pressing buttons one after the other to ensure that everything goes as planned: implacable ("mathematical") logic is not enough, the teams' ability to make syntheses remains essential.

The value of an error, in the sense of usefulness, is obvious in development (it makes processes safer), salutary (except in case of human accidents) if it is discovered very late (the first failure of Ariane 5 was followed by a project review pushed to the extreme for 5 quarters). In some cases, moreover, what is wrongly called an error (including in English), and which is in fact a deviation, is the very basis of the operation of certain systems: this is the case for onboard automatic systems (guidance, flight control, etc.), which is a common feature of launch vehicles.

Systems engineering is enriched by its errors: this is illustrated by the William E. Deming's cycle PDCA: Plan-Do-Check-Act (or Adjust) of the 1950s.

[2] [2] 25 rue Jean Leclaire, 75017 Paris, pfarfal.patsys@sfr.fr